NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

CONTROL CHANNEL VULNERABILITY ANALYSIS OF THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS 802.16M-2011 and 802.16-2009 STANDARDS

by

Chee Meng Tang

September 2012

Thesis Advisor: Su Weilian
Thesis Co-Advisor: Tri Ha

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2012	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE Control Channel Vulnerability Analysis of the Institute of Electrical and Electronics Engineers 802.16m-2011 and 802.16-2009 Standards	**5. FUNDING NUMBERS**
6. AUTHOR(S) Chee Meng Tang	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ___N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

The Institute of Electrical and Electronics Engineers (IEEE) 802.16 set of standards, known as Worldwide Interoperability for Microwave Access (WiMAX), is a family of standards widely deployed for wireless network access. Though WiMAX security vulnerabilities have been extensively analyzed, the IEEE 802.16m-2011 standard incorporates the new advanced air interface (AAI), which is substantially different from legacy standards and justifies reexamination on a clean slate. In this research, the vulnerabilities of IEEE 802.16m-2011 control channels are examined at the medium-access (MAC) and the physical (PHY) layers with proposed attack vectors. Methodologies are proposed to overcome challenges in terms of the timing and power associated with manipulating control channels.

Attacks that manipulate the transmission power of mobile stations are examined in detail, while other attacks on IEEE 802.16m-2011, including multiple-input multiple-output (MIMO) disruption, network-entry disruption, and water-torture are also discussed. Out of fifteen vulnerabilities presented, thirteen were not previously identified for IEEE 802.16m-2011. Existing and new proposed vulnerabilities within legacy standards (specifically IEEE 802.16-2009) are also discussed, including transmission power manipulation, entry procedure attacks, water-torture attacks, and automatic repeat request attacks. Twelve of eighteen vulnerabilities presented were not previously discussed.

14. SUBJECT TERMS WiMAX, Control Channels, IEEE802.16, vulnerabilities	**15. NUMBER OF PAGES** 135
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

CONTROL CHANNEL VULNERABILITY ANALYSIS OF THE INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS 802.16M-2011 and 802.16-2009 STANDARDS

Chee Meng Tang
ME5, Republic of Singapore Navy
Bachelor of Engineering, Nanyang Technological University, 2003

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN ELECTRICAL ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 2012

Author: Chee Meng Tang

Approved by: Associate Professor Weilian Su
Thesis Advisor

Professor Tri Ha
Thesis Co-Advisor

Professor R. Clark Robertson
Chair, Department of Electrical and Computer Engineering

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Institute of Electrical and Electronics Engineers (IEEE) 802.16 set of standards, known as Worldwide Interoperability for Microwave Access (WiMAX), is a family of standards widely deployed for wireless network access. Though WiMAX security vulnerabilities have been extensively analyzed, the IEEE 802.16m-2011 standard incorporates the new advanced air interface (AAI), which is substantially different from legacy standards and justifies reexamination on a clean slate. In this research, the vulnerabilities of IEEE 802.16m-2011 control channels are examined at the medium-access (MAC) and the physical (PHY) layers with proposed attack vectors. Methodologies are proposed to overcome challenges in terms of the timing and power associated with manipulating control channels.

Attacks that manipulate the transmission power of mobile stations are examined in detail, while other attacks on IEEE 802.16m-2011, including multiple-input multiple-output (MIMO) disruption, network-entry disruption, and water-torture are also discussed. Out of fifteen vulnerabilities presented, thirteen were not previously identified for IEEE 802.16m-2011. Existing and new proposed vulnerabilities within legacy standards (specifically IEEE 802.16-2009) are also discussed, including transmission power manipulation, entry procedure attacks, water-torture attacks, and automatic repeat request attacks. Twelve of eighteen vulnerabilities presented were not previously discussed.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

4G	Fourth Generation
A-MAP	Advanced Medium Access Protocol
AAI	Advanced Air Interface
AAS	Advanced Antenna System
ABS	Advanced Base Station
ACK	Acknowledgement
AES-CCM	Advance Encryption Standard (AES)-Counter Mode with Cipher Block Chaining Message Authentication Code (CCM)
AGP	Adaptive Granting and Polling
AGMH	Advanced Generic Medium Access Header
AMS	Advanced Mobile Station
ARQ	Automatic Repeat Request
BE	Best Effort
BS	Base Station
BS_EIRP	Effective Isotropic Radiated Power of Base Station
CID	Connection Identifier
CDM	Code Division Multiplexing
CDMA	Code Division Multiple Access
CMAC	Cypher based Message Authentication Code
CoRe	Constellation Rearrangement
COTS	Commercial Off-the-Shelf
CP	Cyclic Prefix

CPS	Common Part Sublayer
CQI	Channel Quality Indicator
CRC	Cyclic Redundancy Check
CRU	Contiguous Resource Unit
CTC	Convolutional Turbo Code
dB	Decibel
DES	Data Encryption Standard
DL	Downlink
DL-MAP	Downlink Medium Access Protocol
DOCSIS	Data over cable Service Interface Specifications
DRU	Distributed Resource Unit
EAP	Extensible Authentication Protocol
$EIRxP_{IR,min}$	Power (minimum) used for initial ranging
ErtPS	Extended Real-time Packet Service
FCH	Frame Control Header
FDM	Frequency Division Multiplexing
FEC	Forward Error Correction
FFR	Fractional Frequency Reuse
FID	Flow Identifiers
FPC	Fast Power Control
gammaIotFp	Fairness and IoT control factor
GMH	Generic MAC Header

GI	Guard Interval
$G_{overpower}$	Gain for over-powering victim signal
GPS	Global Positioning System
HARQ	Hybrid Automatic Repeat Request
HMAC	Hashed Message Authentication Code
ICV	Integrity Check Value
IE	Information Elements
IEEE	Institute of Electrical and Electronics Engineers
IoT	Interference over Thermal
IS	Intruding System
ISI	Inter-Symbol-Interference
ITU	International Telecommunications Union
$L_{ABS\text{-}IS}$	Loss estimated between ABS and IS
$L_{ABS\text{-}AMS}$	Loss estimated between ABS and AMS
$L_{IS\text{-}AMS}$	Loss estimated between IS and AMS
LBS	Location Based Services
LOS	Line-of-Sight
LRU	Logical Resource Unit
LSB	Least Significant Bit
MAC	Medium Access Control
MAP	Medium Access Protocol
MBS	Multicast and Broadcast Service
MCS	Modulation and Coding Scheme

MIMO	Multiple Input Multiple Output
MS	Mobile Station
MSB	Most Significant Bit
NACK	Negative Acknowledgement
NI	Noise and Interference
NLOS	Near Line-of-Sight
OFDM	Orthogonal Frequency Division Multiplexing
$\text{Offset}_{\text{Initial}}$	Initial Power Offset
$\text{Offset}_{\text{Control}}$	Power offset for control channels
$offsetControl$	Power offset parameter for control channels supplied by BS
$\text{Offset}_{\text{Data}}$	Power offset for data channels
OFDMA	Orthogonal Frequency Division Multiple Access
P-FBCH	Primary Fast Feedback Channel
P-SFH	Primary Superframe Header
PA-Preamble	Primary Advanced Preamble
PDU	Protocol Data Unit
PHY	Physical Layer
$P_{\text{ABS(incident)}}$	Power measured to be incident upon IS
P_{Adjust}	Power adjustment conveyed from BS to MS
$P_{\text{Initial\_Ranging}}$	Power used for initial ranging
$P_{\text{IR,Step}}$	Steps by which power for initial ranging are incremented by
P_{offset}	MS specific transmission power correction factor

PKM	Privacy Key Management
P_{NI}	Estimated average power of NI per sub-carrier at BS
PRBS	Pseudo Random Binary Sequence
$P_{RNG\text{-}ACK}$	Power level adjustment transmitted by BS to MS
PRU	Physical Resource Unit
P_L	Average downlink path loss
P_T	Transmission Power of MS
PTN	Thermal noise power density
P_{TX}	Power to be transmitted by IS
$P_{TX\_IR\_Final}$	Final power transmitted by MS for initial ranging
$P_{TX\_IR\_MIN}$	Initial power transmitted by MS for initial ranging
QoS	Quality of Service
QPSK	Quadrature Phase-Shift Keying
RP	Ranging Preambles
RSS	Received Signal Strength
S-BS	Serving Base Station
S-SFH	Secondary Superframe Header
SA	Security Association
SAP	Service Access Points
SA-Preamble	Secondary Advanced Preamble
SDU	Service Data Unit
SFID	Service Flow Identifier
SINR	Signal-to-Interference plus Noise Ratio

$\text{SINR}_{\text{InitialRanging}}$	Signal-to-Interference plus Noise Ratio for initial ranging
SINR_{min}	Minimum Signal-to-Interference plus Noise Ratio
SINR_{Tgt}	Signal-to-Interference plus Noise Ratio target for normal operation
SIR_{DL}	Signal-to-Interference Ratio for down link
SLPID	Sleep ID
SNR	Signal-to-Noise Ratio
STID	Station Identifier
T-BS	Target Base Station
targetInitialRangingSinr	Constant defined for Initial Ranging
TBCC	Tail-Biting Convolutional Code
TDD	Time Division Duplexing
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
t_{GI}	Guard Time (interval)
Tpropin	Propagation Time (BS to IS)
$t_{\text{prop(max)}}$	Propagation delay (worst case)
TpropMS	Propagation Time (between MS and BS)
Tpropout	Propagation Time (IS to target)
TSTID	Temporary Station Identifier
Tx	Transmit
UGS	Unsolicited Grant Service

UL-MAP	Uplink Medium Access Protocol
WiMAX	Worldwide Interoperability for Microwave Access

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Introduction. Worldwide Interoperability for Microwave Access (WiMAX) is a next-generation wireless data-communications standard poised to dominate mobile data connectivity in the commercial and military arenas. However, the security and robustness of the commercial standard need to be examined and risks mitigated before they can be considered for military applications. At the same time, with the proliferation of WiMAX networks worldwide, the ability to exploit or disrupt operations can be of operational worth.

Related Works. Much work has been accomplished to evaluate security concerns and vulnerabilities within the IEEE 802.16 standards. The majority of works reviewed, including [1], [2], [3], [4], [5], [6] and [7], exploited WiMAX Media Access Control (MAC) management/control messages that were not authenticated or encrypted, giving rise to man-in-the-middle attack vulnerabilities.

The release of IEEE 802.16m-2011 saw a substantially revised MAC and physical (PHY) layers in the form of the advanced air interface (AAI), which essentially can be likened to a new standard built to run in harmony with previous legacy standards. This fundamentally new interface warrants a fresh examination for vulnerabilities, and Blair [8] performed such an examination. He highlighted vulnerabilities related to the lack of authentication for ranging and capability negotiation messages, which are exchanged prior to execution of the authentication process. An attacker can spoof a ranging response message with abort flag set to deny entry to mobile stations (MSs). Alternatively, capability negotiation messages can be altered to cause a low security connection to be formed to compromise data sent during the session.

In this thesis, methods of manipulating the WiMAX control channel for both IEEE 802.16m-2011 and the legacy IEEE 802.16-2009 are explored**.**

MAC Management Messages. MAC management messages are a key part of WiMAX control channels and are secured by two types of protection. The integrity check value (ICV) affords complete protection, including confidentiality, integrity, and authenticity, first introduced with IEEE 802.16m-2011. Cypher-based message authentication code (CMAC) and hashed message authentication code (HMAC) provides authenticity and integrity protection but no encryption. For these to be used, a security association needs to be established, which includes authentication as well as key exchange. While ICV and CMAC/HMAC were extended to more and more control messages over the years, there are still messages that remain unprotected.

Spoofing and Injection of Control Messages. Most vulnerabilities involve an intruding station (IS) spoofing false MAC management messages at the ABS or an AMS. In contention-based wireless standards such as IEEE 802.11 (Wifi), knowing the frequency as well as key parameters is sufficient for an attacker to start injecting messages. The time-division multiple access (TDMA) and orthogonal frequency-division multiplexing (OFDMA) nature of WiMAX means that, on top of knowing normal parameters, transmitting on the correct sub-carriers and at the correct timing is also crucial. Most literature discusses vulnerabilities of MAC management messages assuming they can be injected successfully without discussing details. Boom correctly identified that the single biggest challenge in mounting attacks on TDMA systems is timing [9].

The challenges and proposed solutions for injecting MAC management messages, both at advanced base stations (ABSs) and advanced mobile stations (AMSs), are examined in detail in this thesis. The attacker will first need to attain downlink synchronization by detecting and decoding preambles. The connection identifiers (CID) of targeted AMS need to be acquired by listening to the AMS when it joins the network. The downlink medium access protocol (DL-MAP) and uplink medium access protocol (UL-MAP), which contain resource allocations for each frame, need to be decoded. The attacker can then know when and which sub-carriers to inject the formulated messages. IEEE802.16m-2011 scrambles assignment MAPs for unicast messages, leaving only broadcast messages that can be located and exploited.

Several different scenarios exist, depending on whether we are injecting on the uplink (to the BS) or the downlink (to the MS) and whether location of the subject is known. The timing for injected messages needs to be referenced to the ABS, which means propagation delay from the attacker to the subject (including their relative positions) needs to be factored in, and transmission timing advanced or retarded if necessary. If the subject's precise location is known, timing and power adjustments can be estimated from the distances among the attacker, BS, and MS. If the location of the MS that we plan to inject messages into is unknown, we can attempt transmission of an injected message over multiple attempts over a selected range bounded by the cell's dimension until the transmission commencement falls within the guard interval window. If injecting into an uplink, the attacker can use the initial ranging process to obtain the precise timing, frequency, and power adjustments required to obtain a nominal signal at the BS.

As the formulated signal needs to overcome a real signal, the power incident upon the subject needs to be sufficiently higher. The attacker's transmission power is thus targeted to be higher than the nominal signal by the signal-to-noise ratio (SNR) requirement for the modulation scheme.

Formulated message need to take the effects of automatic repeat request (ARQ) into consideration, incorporating sequence numbers as well as being longer than a ARQ block to ensure that the cyclic redundancy check (CRC) test passes and the message is accepted.

The position uncertainty of the MS, BS, and attacker and the corresponding variations in propagation delay were analyzed against the guard interval (GI) between OFDM symbols. It was found that the guard interval is more than sufficient to handle uncertainties foreseen.

Power Related Attacks on IEEE 802.16m-2011. Having proposed the means to inject MAC management messages, we proceed to discuss a class of attack that involves injecting messages to manipulate the uplink power control of AMSs. One possibility of attacking uplink power management is to inject an uplink noise and interference level broadcast (AAI-ULPC-NI) message with a low or high noise and interference (NI) value. If a low value is injected, the AMS transmission power drops and its bit error rate increases—or reception may be eliminated altogether. If a high NI value is injected, the high signal strength may increase interference for cells in the vicinity using the same frequencies. AAI-ULPC-NI is a broadcast message, and all AMSs within the cell served by the ABS can be affected. Although all AMSs can potentially be affected, timing adjustment from attacker to individual AMSs also needs to be correct for the AMS to take in the broadcast correctly.

In another possibility for attacking uplink power management, the SINRtgt parameter might be manipulated by spoofing a system configuration descriptor (AAI-SCD) message with amended “dataSinrMin”, “gammaIotFpx” and “alpha” parameters.

Other Attacks on IEEE 802.16m-2011. Multiple input multiple output (MIMO) parameters can be doctored to disrupt network operations. By spoofing the AAI-SCD message with a false "Alpha" parameter (which indicates the number of receive antennas), an AMS attempting to join a network can possibly be confused as to the actual number of receive antennas on the ABS and adopt the wrong MIMO scheme as well as the wrong parameters and codes, disrupting communications. Another attack vector involves spoofing the AAI-SBC-REQ message during initial network entry, indicating lower or erroneous MIMO parameters. Alternatively, an AAI-SBC-RSP management message can be spoofed with MIMO settings that do not match those requested by AMS. As a result, a mismatch in parameters between ABS and AMS can arise that can disrupt communications.

The ABS can be flooded to deny service to legitimate AMSs. Repeated transmission of AAI-RNG-REQ messages can tie up ABS resources and deny entry for legitimate AMSs. During network entry, by injecting AAI-RES-CMD before security association is formed by the targeted AMS, an attacker can cause the AMS to abort the process and reset its MAC.

An AMS in sleep mode to conserve battery power can be forced to be awake longer than necessary by an attacker spoofing AAI-TRF-IND, thus, draining its battery faster. This vulnerability has been identified in legacy systems in [2], [4], and [5] and is verified as still present within IEEE 802.16m-2011. Alternatively, AMSs in idle mode to conserve power can be forced to join a network by an attacker spoofing AAI-PAG-ADV, also draining its battery faster.

An AAI-RNG-ACK message can be spoofed with incorrect timing, frequency, and power adjustments to disrupt network entry.

Blair proposed spoofing AAI-SBC-REQ with a low or nil encryption/ decryption capability class [8]. Alternatively, an attacker can issue an AAI_SBC-RSP management message with capability classes that do not match those requested by the AMS.

An attacker can spoof AAI-NBR-ADV with a nonexistent BS or by falsely reporting poor characteristics of neighboring BSs to hamper MSs from initiating handover to a BS with better characteristics. This vulnerability was identified for the legacy standard [2, 5] and was found to still exist in IEEE 802.16m.

An AAI-LBS-ADV message can be spoofed with wrong latitude and longitude coordinates for the serving and neighboring ABSs to confuse an AMS as to its own location and degrade its GPS receiver's performance.

Attacks on Legacy Systems. An AAS_Beam_Select message can be spoofed to inform the BS of a preferred beam radically different from that previously selected to disrupt communications.

By spoofing an FPC message, the attacker can reduce or increase the MS transmission power over a range of +32 dB to -32dB, in steps of 0.25 dB [5].

All ARQ messages are unprotected and can be leveraged to disrupt communications. ARQ-Reset, ARQ-Discard, and ARQ Feedback can be spoofed to misalign ARQ sequences between the BS and MS. The vulnerability of ARQ-Reset is identified in previous literature [3].

PRC-LT-CTRL message can be spoofed to turn on/off long-term MIMO precoding with feedback and to change precoding application delay with the objective of causing a mismatch between the BS and MS, disrupting communications.

The BS can be flooded to deny service to legitimate MSs. Repeated transmission of RNG-REQ messages can tie up ABS resources and deny entry for legitimate MSs. During network entry by victim AMSs, by injecting RES-CMD before the security association is formed, an attacker can cause the MS to abort the process and reset its MAC.

MSs in sleep mode can be forced to wake up sooner than necessary, thus draining their battery faster by spoofing MOB-TRF-IND [2], [4], and [5]. As for MSs in idle mode, they can be forced to join a network by an attacker's spoofing MOB-PAG-ADV to drain the battery.

An attacker can spoof MOB-NBR-ADV with a nonexistent BS or by falsely reporting poor characteristics of neighboring BSs to hamper MSs from initiating handover to a BS with better characteristics [4, 5].

The UCD, DCD, UL-MAP, and DL-MAP together serve to define the UL and DL channels. Modification or scrambling of these unprotected management messages will result in disruption of communications.

An attacker can spoof DBPC-REQ to request a BS to change its communication profile to one with a higher data rate but less robustness, i.e., a profile unsuitable for prevailing channel conditions. This can result in high error rates, disrupting communications [5].

An attacker may spoof CLK-CMP messages to misalign MS/BS clocks.

Conclusion. While IEEE 802.16-2009 offered significant improvements over its predecessors, a number of control messages still remain unauthenticated and unencrypted. In addition to the vulnerabilities identified in the literature, twelve attack vectors using control messages are proposed in this thesis.

IEEE 802.16m-2011 is a significant revision (with a new set of control messages), structurally enhanced to increase privacy and raise barriers to attacks while maintaining backward compatibility with legacy standards. By introducing encryption for some control messages, the new standard reduces the exposure of system operating information that may be used against it. More significantly, by scrambling the advanced medium access protocol (A-MAP) using secret initial vectors exchanged securely during security negotiations upon network entry, the passive listener will have difficulty identifying how radio resources are allocated or destination and originator AMS. This effectively prevents exploitation of all unicast control messages and enhances privacy. Nonetheless, broadcast control messages are still open to exploitation, and a significant number of vulnerabilities in IEEE 802.16-2009 still exist in this revision. In addition to the vulnerabilities identified in the literature, thirteen attack vectors using control messages are proposed in this thesis.

References

[1] K. Scarfone, C. Tibbs, and M. Sexton, “Guide to securing WiMAX wireless communications,” *National Institute of Standards and Technology Special Publication* 800–127, 2010.

[2] T. Han, N. Zhang, K. Liu, B. Tang, and Y. Liu, "Analysis of mobile WiMAX security: Vulnerabilities and solutions," *Proc. 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems,* pp. 828–833, Sept. 2008.

[3] K. Bakthavathsalu, S. Sampalli, and Q. Ye, "Management frame attacks in WiMAX networks: Analysis and prevention," *2010 Seventh International Conference On Wireless and Optical Communications Networks (WOCN),* pp. 1–7, Sept. 2010.

[4] A.M. Taha, A.T. Abdel-Hamid, and S. Tahar, "Formal analysis of the handover schemes in mobile WiMAX networks," *2009 IFIP International Conference on Wireless and Optical Communications Networks (WOCN),* pp.1–5, April 2009.

[5] A. Deininger, S. Shinsaku, J. Kurihara, and T. Tanaka, "Security Vulnerabilities and Solutions in Mobile WiMAX" *International Journal of Computer Science and Network Security*, vol. 7, no. 11, November 2007.

[6] A.K.M.N. Sakib and M.M.S. Kowsar, "Shared key vulnerability in IEEE 802.16e: Analysis & solution," *2010 13th International Conference on Computer and Information Technology (ICCIT),* pp. 600–605, Dec. 2010.

[10] M.S. Rahman and M.M.S. Kowsar, "WiMAX security analysis and enhancement," *2009 12th International Conference on Computers and Information Technology (ICCIT),* pp. 679–684, Dec. 2009.

[11] B. Blair, “A Vulnerability Analysis of the Institute of Electrical and Electronics Engineers 802.16M-2011 Standard at the Air Interface” M.S. thesis, Naval Postgraduate School, Monterey, CA, March 2011.

[12] D. Boom, “Denial of service vulnerabilities in 802.16 wireless networks,” M.S.thesis, Naval Postgraduate School, Monterey, CA, September 2004.

ACKNOWLEDGMENTS

I would like to acknowledge the patience and support of my loving wife, Pei Gek, who looked after the needs of my kids while I spent days and nights on the thesis and schoolwork.

Professor Su and Professor Ha, your reassurance, guidance, and encouragement made this journey worthwhile.

Donna Miller, thank you for facilitating a conducive work environment for us.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

The last three decades saw phenomenal growth in terms of information technology, and, in tandem, telecommunications and networks. In this information age, the generation, processing, distribution, and consumption of information drives numerous aspects of warfare, business, and everyday life. The proliferation of the Internet's reach and the explosion of online content has driven demand for mobile data communications. On the commercial front, we have seen tremendous leaps from low-speed, low-mobility capabilities to third-generation broadband, with market penetration outstripping that of landline phones in many countries.

Worldwide Interoperability for Microwave Access (WiMAX) is a next-generation, wireless data-communications standard poised to dominate mobile data connectivity in the commercial and military arenas. Numerous WiMAX networks are deployed worldwide (see Figure 1). WiMAX Forum states that WiMAX subscriptions exceeded 20 million in 2011, with more than $502 million spent on WiMAX equipment in Quarter 1 of 2011 alone [1]. Meanwhile, population coverage has broken through the 800 million mark (see Figure 2) and is fast approaching a billion [2].

On the military front, developments in network-centric warfare, unmanned vehicles, and sensor networks have driven the capability development and bandwidth requirements of mobile-data connectivity. Cost and budgetary pressures in the developed world have caused defense budgets to be pared and militaries to leverage commercial technologies more and more, resulting in shifts to commercial, off-the-shelf (COTS) technologies, including in wireless networks.

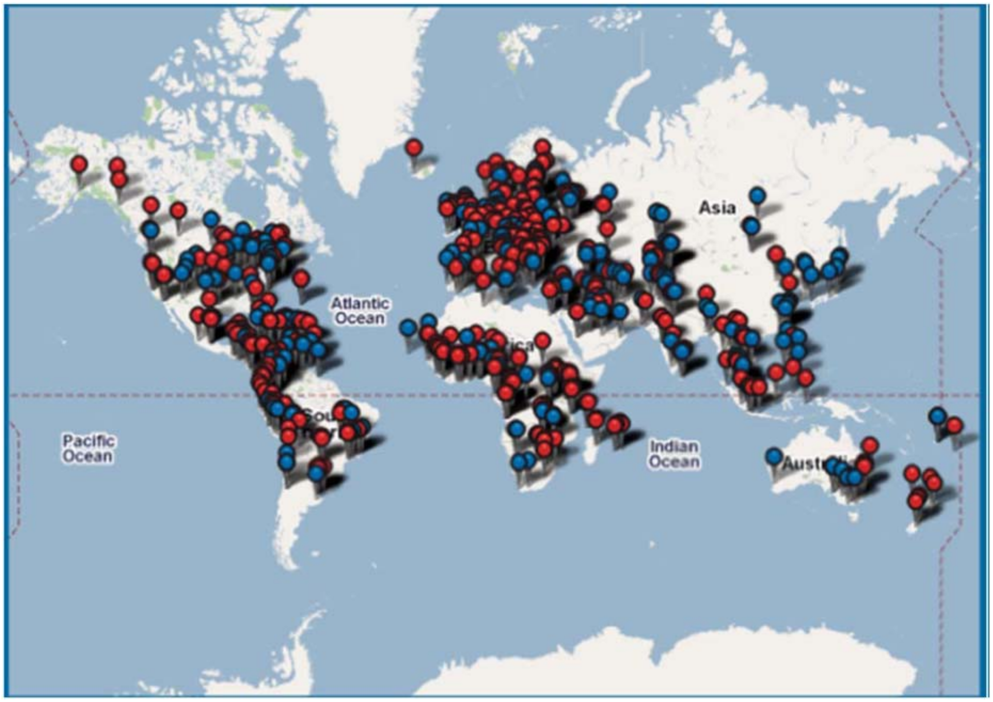


Figure 1. Pictorial representation of WiMAX deployments (From [3]).

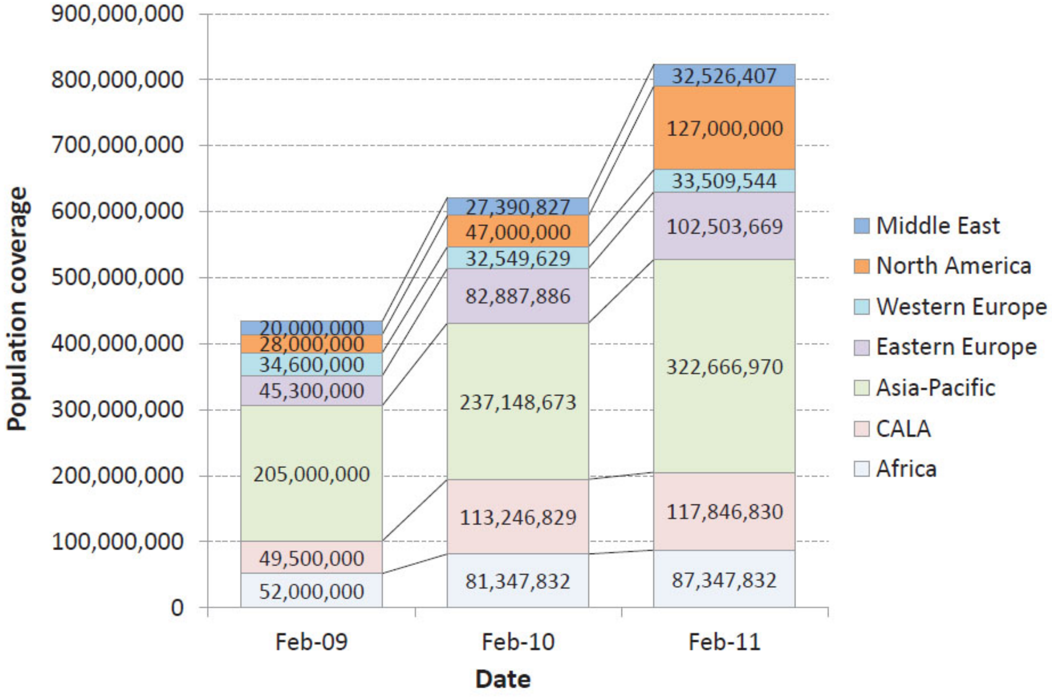


Figure 2. Population coverage of WiMAX deployments [2].

However, the security and robustness of the commercial standard must be examined and the risks understood and mitigated before it can be considered for military applications. At the same time, with the proliferation of WiMAX networks worldwide, the ability to exploit or disrupt operations can be of operational value.

B. WIMAX STANDARD DEVELOPMENT

The IEEE 802.16 group of standards had its beginnings in 1998, when a group was formed to develop the fourth generation of air-interface standards for wireless broadband. The initial standard had a single-carrier, physical layer operating from 10 GHz - 66 GHz for line-of-sight (LOS) operations, with many MAC-layer concepts adapted from the cable modem DOCSIS (data over cable service interface specifications) standard.

Orthogonal frequency-division multiplexing (OFDM) was subsequently incorporated to mitigate multipath fading, and operating frequencies of 2–11 GHz were adopted to enable near line-of-sight (NLOS) operations instead of LOS.

Orthogonal frequency-division multiple access (OFDMA) was another key feature adopted later, resulting in IEEE 802.16-2004, which, forming the first baseline standard, superseded all previous versions. Up to this point, all standards were designed for fixed or nomadic applications. IEEE 802.16e was developed and released in 2005, providing support for mobile nodes and incorporating new security features.

The next key milestone was IEEE 802.16-2009, which includes important enhancements such as support for 20 MHz bandwidth, improved multi-antenna transmission and processing schemes, and enhanced multicast, broadcast, and location-based services. Within IEEE 802.16m-2011, the advanced air interface (AAI) was developed to meet the requirements of ITU-R/IMT-Advanced for 4G systems. Relying on available bandwidth and multi-antenna mode, IEEE 802.16m systems are now capable of over-the-air transfer rates in excess of 1 Gbit/sec while maintaining interoperability with legacy equipment built to preceding standards.

C. RELATED WORK

Much work has been accomplished to evaluate security concerns and vulnerabilities within IEEE 802.16 standards. Some of these concerns are discussed in the following subsections.

1. Lack of Encryption and/or Authentication for MAC Management/ Control Messages

The vast majority of works reviewed, including [4], [5], [6], [7], [8], [9] and [10], exploited WiMAX MAC management/control messages that were not authenticated or encrypted, giving rise to man-in-the-middle attack vulnerabilities.

Han et al. in [5] as well as Rahman et al. in [10] exploited the fact that even with newer versions of legacy WiMAX (up to IEEE 802.16-2009), which offered authentication for selected management messages, the initial ranging process (part of the network entry process) was not protected. Hence, an attacker could modify management messages and force a low security configuration for the network session. Similar vulnerabilities also provided avenues for an attacker to modify unprotected messages to trigger an abortion of the ranging process, hence aborting network entry. Lack of authentication of sleep mode messages was also exploited to trigger mobile stations to enter sleep mode.

Bakthavathsalu et al. in [6] leveraged similar weaknesses to spoof unprotected messages within network entry authentication processes to force MSs entering the network into authorization wait states, disrupting network entry processes. Even after network entry, unauthenticated ARQ messages could also be spoofed to reset ARQ sequence numbers at MSs, disrupting communications.

Taha et al. in [7], as well as Andreas in [8], highlighted the same lack of authentication, which can lead to water-torture attacks in which sleeping MSs are forced to wake up by an attacker injecting traffic indication messages, indicating the presence of messages awaiting the sleeping MS. In addition, attackers could falsify neighbor advertisement messages to disrupt the handover process.

Deininger et al. in [8] went on to discuss related security weaknesses valid for IEEE 802.16-2009 and earlier. The fast power control message (FPC) can be altered to increase or decrease the power of MSs. Messages can be spoofed to remove MSs from multi-cast polling groups. An MS can also be force into a downlink burst profile not suitable for its operating environment, adversely affecting error rates and throughput. Power control mode can also be manipulated.

2. Weakness of Symmetrical Keys for Multicast/Broadcast

Deininger et al. in [8] also discuss the inherent weakness of using symmetrical keys for multicast and broadcast. For practical considerations and efficiency, the same set of symmetrical keys is used for all BSs and MSs for encryption and decryption of multicast and broadcast traffic. However, this means that if one node is compromised, all multicast and broadcast traffic is compromised.

3. Weakness in Encryption Algorithm

According to [4], IEEE 802.16-2004 supports only the data encryption standard (DES), for which weaknesses have been uncovered and which is deemed less secure. IEEE 802.16e-2005 includes support for the advanced encryption standard (AES), which resolved this issue, and, for the time being, is deemed secure enough for the federal government to use to protect sensitive data.

4. Progressive Elimination of Security Gaps

The persistent and good work of the above researchers prompted review of and incremental improvements in protection for later versions of the standard through selective introduction of authentication for management messages. Thus, some of the vulnerabilities seen in the past have been removed in revisions of WiMAX.

5. New AAI Interface for IEEE 802.16m Warrants Fresh Vulnerability Assessment on a Clean Slate

The release of IEEE 802.16m-2011 saw a substantially revised MAC and PHY in the form of the advanced air interface (AAI), which can be likened to a new standard built to run in harmony with previous legacy standards. This fundamentally new interface warrants a fresh examination for vulnerabilities, and Blair [11] performed such an examination. He highlighted vulnerabilities related to the lack of authentication for ranging and capability negotiation messages that are exchanged before execution of the authentication process. An attacker could spoof ranging response messages with the abort flag set to deny entry to MSs. Alternatively, capability negotiation messages could be altered to cause a low security connection to be formed to compromise data sent during the session.

D. RESEARCH OBJECTIVE

This project involves exploring methods of hacking into and manipulating the WiMAX control channel**.** This thesis research can serve as a starting point to protect, as well as to exploit, protocol weaknesses in WiMAX, thus opening exploitation space.

E. RESEARCH SCOPE

The focus of this research is on IEEE 802.16m-2011, which, besides offering advanced capabilities, extends support for all legacy standards. Coverage on the legacy standard IEEE 802.16-2009 is included when relevant and appropriate.

The system boundary is set at interactions within a cell supported by an advanced base station and its sectors where applicable. For the purposes of this research, we limit ourselves to the time-division duplexing (TDD) configuration for WiMAX deployment, as this is by far the most popular configuration deployed.

F. ORGANIZATION

A brief overview of the IEEE 802.16m-2011 and IEEE 802.16-2009 are presented in Chapter II to form a foundation for later material. Protection schemes in WiMAX for control messages and the extent of their coverage are introduced in Chapter III. Investigation efforts are thus focused on unprotected messages. In Chapter IV, the methodology for spoofing control messages within a challenging time-division multiple access (TDMA) regime is proposed. With the target and tools identified, previously identified attack vectors for IEEE 802.16m-2011 and legacy standards are discussed and new attack vectors are proposed in Chapter V. Conclusions and suggested future work are presented in Chapter VI.

THIS PAGE INTENTIONALLY LEFT BLANK

II. IEEE 802.16M-2011 - ADVANCED AIR INTERFACE

An overview of the IEEE 802.16m-2011 standard is presented in this chapter to form a basis for discussion in subsequent chapters. Emphasis is placed on concepts relevant to this research topic. An overview is first provided with reference model and state diagrams, to form a context and foundation. Subsequently, MAC and PHY functions are dealt with in detail. Although this research covers IEEE 802.16-2009, in the interests of space, an overview is not provided, though relevant differences are highlighted when discussing vulnerabilities.

A. OVERVIEW

The reference model of the IEEE 802.16m-2011 standard is shown in Figure 3; it is defined in line with the open systems interconnection (OSI) model. The standard's scope, however, is limited to the MAC and PHY layer.

The MAC layer consists of three sublayers, the service specific convergence sublayer (CS), the MAC common part sublayer (CPS), and the security sublayer. The service specific CS provides transformation and mapping of network layer data into MAC service data units (SDU), as well as header suppression functions. Different CSs are provided for different network layer protocols. The MAC CPS contains the core functionality of the standard, including system access, bandwidth allocation, connection establishment, and connection maintenance. The security sublayer performs authentication, secure key exchange, and encryption functions.

The interfaces between layers are defined as service access points (SAP), with data entering a sublayer referred to as service data unit (SDU) and data leaving a sublayer defined as protocol data unit (PDU).

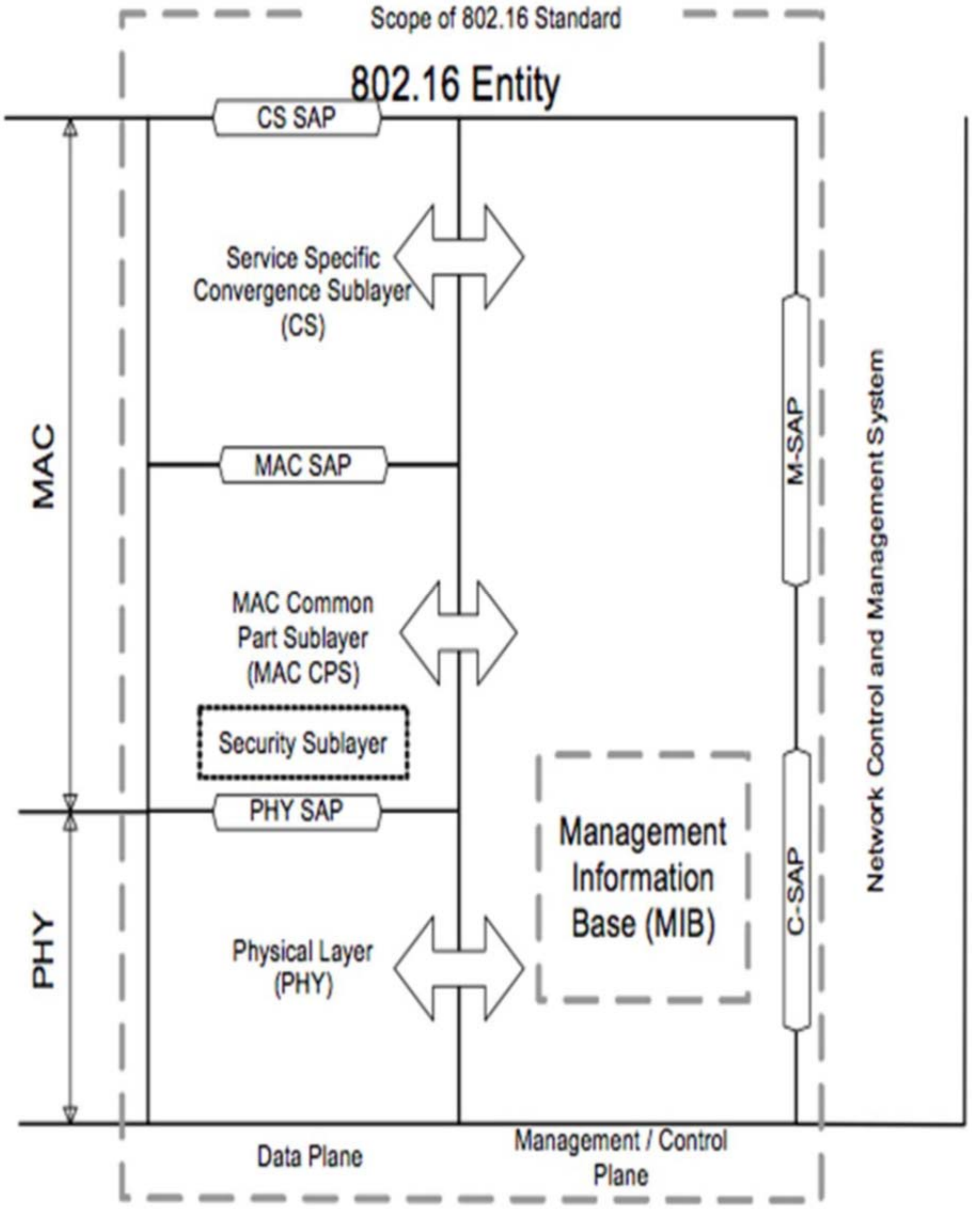

Scope of 802.16 Standard
802.16 Entity
CS SAP
Service Specific Convergence Sublayer (CS)
MAC SAP
MAC Common Part Sublayer (MAC CPS)
Security Sublayer
PHY SAP
Physical Layer (PHY)
MAC
PHY
M-SAP
C-SAP
Management Information Base (MIB)
Network Control and Management System
Data Plane
Management / Control Plane

Figure 3. Reference model for IEEE 802.16 (From [13] section 1.4).

The contents of the protocol stack are illustrated in Figure 4.

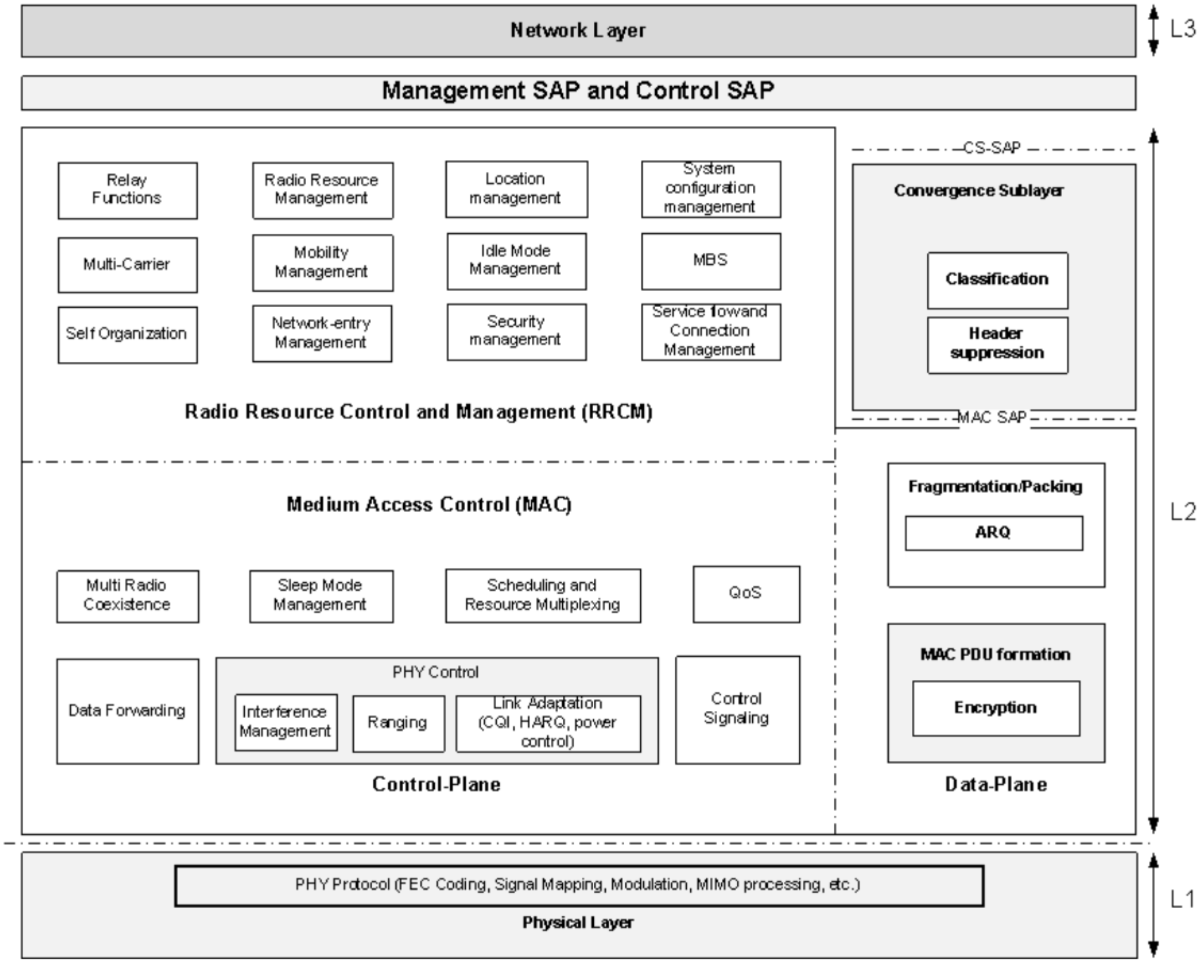


Figure 4. IEEE 802.16m general protocol stack (From [14]).

The radio resource control and management group include a number of functional blocks. The radio resource management block adjusts radio network parameters according to load and environment. The mobility management block monitors neighboring base stations (BSs) and makes handover decisions. The network entry management block controls network entry procedures and sequences. The location management block manages location-based services (LBS). The idle mode management block controls idle mode operation. The security management block performs key management. The system configuration block manages system configuration and generates broadcast control messages such as superframe headers. The multicast and broadcast service (MBS) block controls and generates MBS messages. The service flow and connection management block manages and allocates station identifiers (STIDs) and flow identifiers (FIDs). The multi-carrier block allows a single MAC to control multiple physical layers.

The medium access control (MAC) function group on the control plane consists of a number of functional blocks. The PHY control block performs signaling such as ranging, channel quality measurement/ feedback (CQI), and hybrid automatic repeat request (HARQ) ACK or negative acknowledgement (NACK) signaling. The control signaling block generates resource allocation messages such as advanced medium access protocol (A-MAP) and control messages. The sleep-mode management block oversees sleep operations and is responsible for related messages. The quality-of-service block manages data rate according to quality-of-service (QoS) inputs from connection management block. The scheduling and resource-multiplexing block schedules and multiplexes data based on requirements and subchannel characteristics. The interference management block performs inter-BS coordination as well as intra-BS measures to manage interference.

The medium access control function group on the data plane consists of a number of functional blocks. The fragmentation/packing block fragments and packs MAC SDU based on inputs from scheduling and resource multiplexing block. The automatic repeat request (ARQ) block generates sequentially numbered ARQ blocks from MAC SDUs from the same flow. The MAC protocol data unit formation block constructs MAC PDUs.

The state diagram of an IEEE 802.16m mobile station is provided in Figure 5.

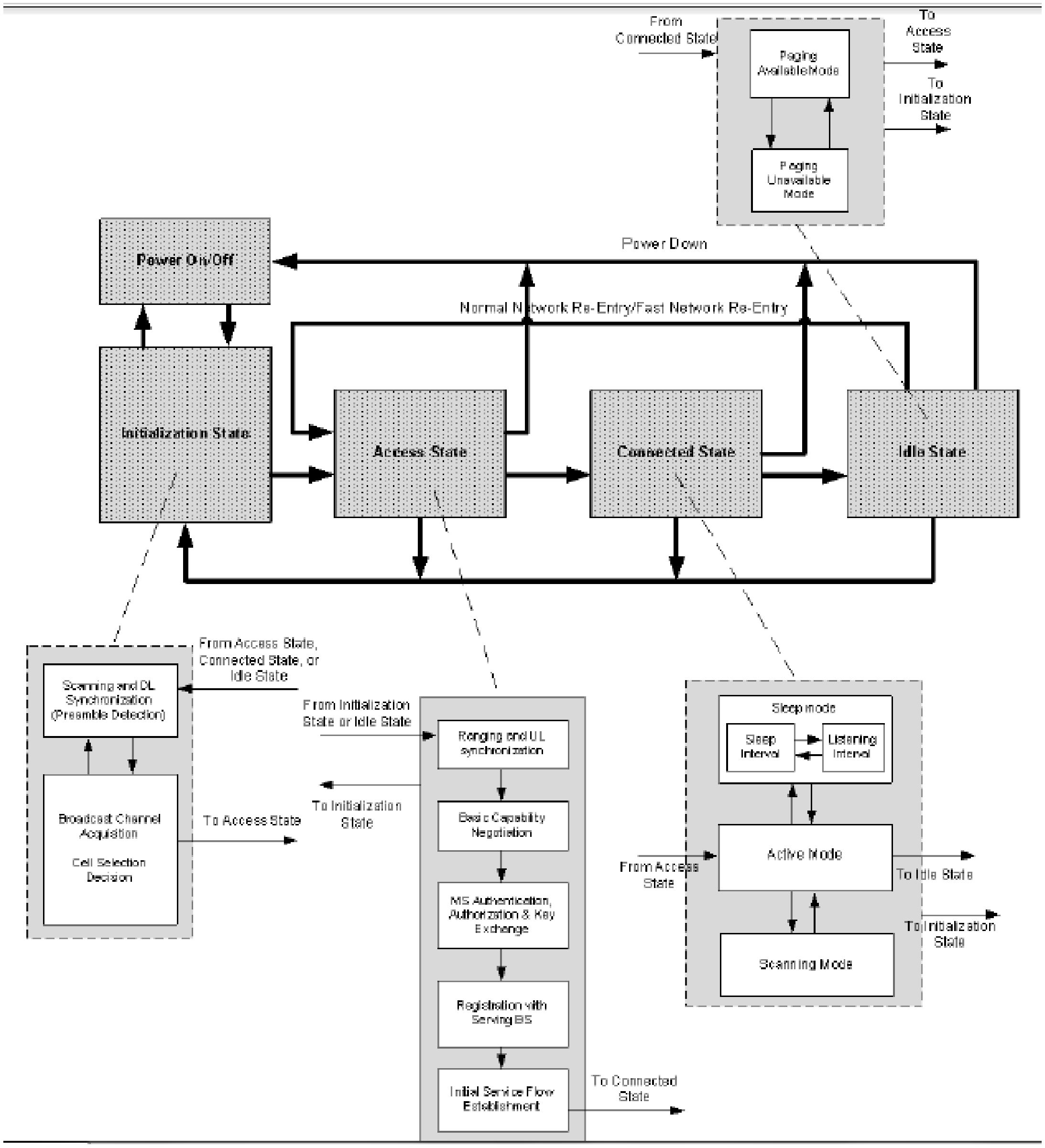

From Connected State
Paging Available Mode
Paging Unavailable Mode
To Access State
To Initialization State
Power On/Off
Power Down
Normal Network Re-Entry/Fast Network Re-Entry
Initialization State
Access State
Connected State
Idle State
From Access State, Connected State, or Idle State
Scanning and DL Synchronization (Preamble Detection)
Broadcast Channel Acquisition
Cell Selection Decision
To Access State
From Initialization State or Idle State
To Initialization State
Ranging and UL synchronization
Basic Capability Negotiation
MS Authentication, Authorization & Key Exchange
Registration with Serving BS
Initial Service Flow Establishment
To Connected State
Sleep mode
Sleep Interval
Listening Interval
From Access State
Active Mode
To Idle State
To Initialization State
Scanning Mode

Figure 5. IEEE 802.16m mobile station state transition diagram (From [14]).

During initialization state, mobile station without active connections scans and synchronizes to cell, acquiring cell identification and system configuration information.

During access state, mobile station performs network entry through ranging and uplink synchronization, capability negotiation, authentication, authorization and key exchange, registration, and service flow establishment.

During connected state, mobile station performs uplink and downlink communications with the following sub-modes: active mode, sleep mode and scanning mode. Active mode is the mode where normal communications occur. On downlink communications, channel quality measurements are performed by the MS. These measurement results are sent to the BS for the BS scheduler to adapt its uplink and downlink assignments to channel conditions. Sleep mode is used by the MS to minimize power drain and radio resources. Traffic indication message from the BS alerts the sleeping MS that a message is incoming. Scanning mode is used by the MS to prepare for handover. The MS can be instructed to enter this mode, where the MS scans for other BSs.

During idle state, the MS becomes unregistered and is only able to receive downlink broadcasts. If pre-negotiated with paging available, the MS can be paged, causing it to enter access state for network reentry.

B. MEDIA ACCESS LAYER

1. Addressing

All mobile terminals are uniquely identified by a 48-bit universal MAC address. Within the IEEE 802.16-2009, all connections are uniquely identified by 16-bit connection identifiers (CIDs). With the IEEE 802.16m-2011, there are two addressing identifiers instead of the CID (Figure 6): the station identifier (STID), which is 12-bits long and used to identify an AMS; and the flow identifier (FID), which is 4-bits long and used to address active service flows of an AMS.

STID (12 bits)	FID (4 bits)

Figure 6. Illustration of IEEE 802.16m.2011 addressing.

This enables greater efficiency, as the advanced generic medium access header (AGMH) for MAC PDUs need only contain FIDs, while the STIDs need only be included within the assignment advanced medium access protocol (A-A-MAP), which maps out radio resources (in terms of sub-carriers and time) as bursts for individual AMS.

2. MAC Headers

The AGMH is used with MAC management messages or with user payload (see Figure 7). This header is significantly smaller than legacy headers due to the removal of CID (16 bits), which is replaced with FID (four bits). Extended headers can be added as required, while MAC signaling headers do not carry user payload but are used for control and management signaling. These include bandwidth request, reports, and feedback functions.

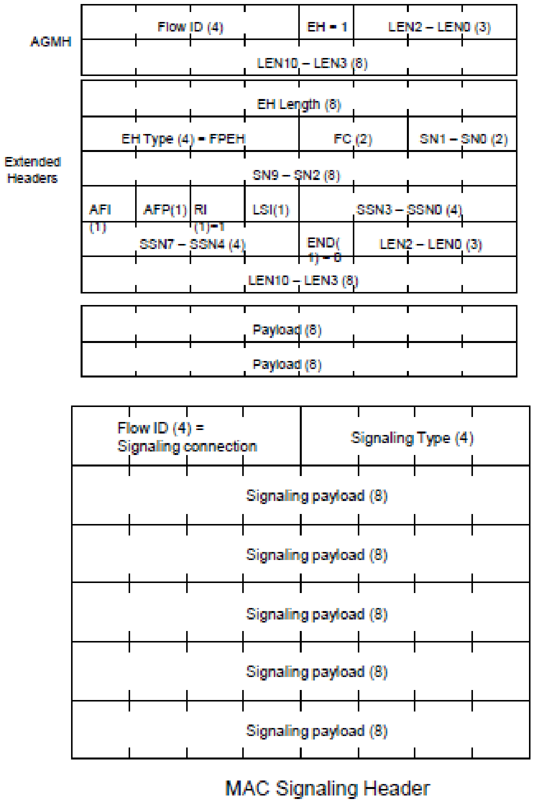


Figure 7. MAC headers and extended headers (From [14]).

3. Mobility Management and Handover

Handover can be AMS initiated or ABS initiated. A series of MAC management messages are sent over the air, as well as the backhaul (between serving base station and target base station). In both cases, the serving base station (S-BS) sends a HO-REQ message to the target base station (T-BS), which replies with a HO-RSP to the S-BS. If handover can proceed, S-BS issues an AAI-HO-CMD message to the AMS. The AMS then replies with an AAI-HO-IND message before commencing a network reentry procedure with T-BS. Upon completion, T-BS sends HO-COMPLT to S-BS. This process is illustrated in Figure 8.

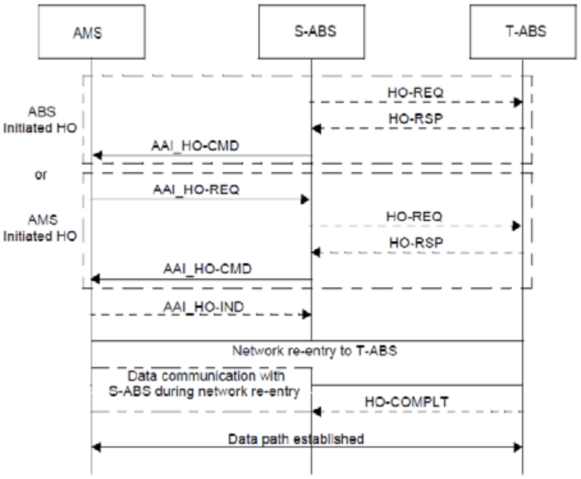
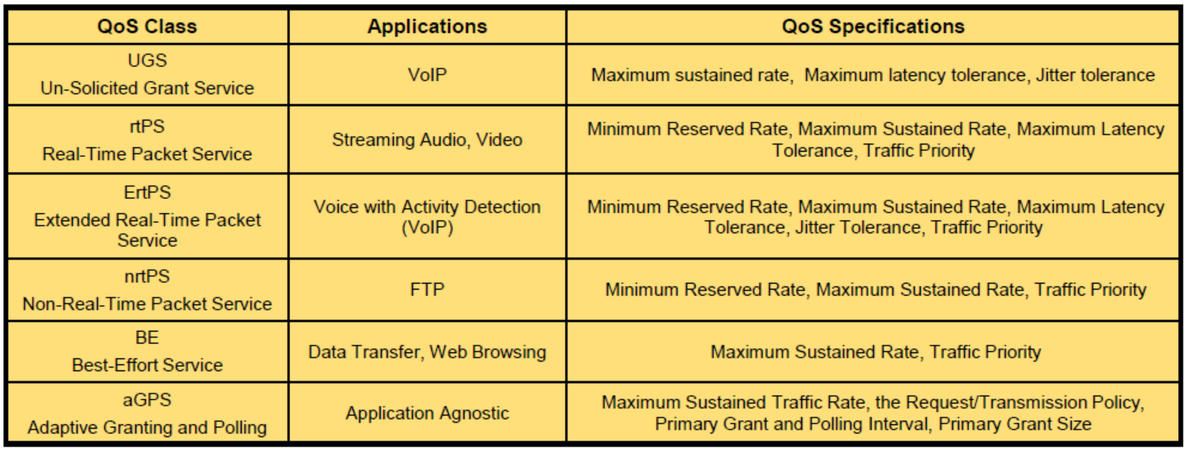


Figure 8. General handover flow (From [14]).

4. Quality of Service

A unidirectional flow of user data packets is associated with a service flow identifier (SFID), which in turn has an associated QoS. The QoS represents the tradeoff and prioritization of resources to ensure a satisfactory level of experience by different applications and users of the system. QoS classes range from unsolicited grant service (UGS) meant for providing fixed and constant bandwidth for real-time applications (much like dedicated circuits) to best effort (BE), which supports non-time-sensitive applications. A summary of QoS classes available for use is given in Table 1.

Table 1. QoS classes.



QoS Class	Applications	QoS Specifications
UGS Un-Solicited Grant Service	VoIP	Maximum sustained rate, Maximum latency tolerance, Jitter tolerance
rtPS Real-Time Packet Service	Streaming Audio, Video	Minimum Reserved Rate, Maximum Sustained Rate, Maximum Latency Tolerance, Traffic Priority
ErtPS Extended Real-Time Packet Service	Voice with Activity Detection (VoIP)	Minimum Reserved Rate, Maximum Sustained Rate, Maximum Latency Tolerance, Jitter Tolerance, Traffic Priority
nrtPS Non-Real-Time Packet Service	FTP	Minimum Reserved Rate, Maximum Sustained Rate, Traffic Priority
BE Best-Effort Service	Data Transfer, Web Browsing	Maximum Sustained Rate, Traffic Priority
aGPS Adaptive Granting and Polling	Application Agnostic	Maximum Sustained Traffic Rate, the Request/Transmission Policy, Primary Grant and Polling Interval, Primary Grant Size

5. MAC Management / Control Messages

MAC management/control messages form an important part of the many control channels. Messages are put into PDUs and transported over broadcast or unicast connections. Hybrid automatic repeat request (HARQ) is used for MAC messages sent over unicast control connections. Some of these message types are encrypted and protected with integrity check value (ICV) and some are authenticated with cypher-based message authentication code (CMAC), while others are not protected. An entirely new set of messages (besides legacy ones that are still supported) is defined for IEEE 802.16m-2011, which is prefixed with "AAI."

6. Connection and Session Management

In IEEE 802.16m-2011, connections are identified by a combination of STID (12 bits) and FID (four bits). Management connections carry MAC management messages and are bidirectional, which is established upon successful registration of AMS. Transport connections carry user data and are unidirectional.

Service flows are created through the dynamic service addition/change/delete family of MAC control messages with QoS associated. These service flows are uniquely mapped to FIDs.

In IEEE 802.16-2009, a connection is identified by a 16-bit connection ID (CID) and are all unidirectional. The three types of management connections are basic (for short and time-sensitive MAC messages), primary (for long and delay-tolerant MAC messages), and secondary.

7. Mobility and Power Management

The vast majority of WiMAX devices are mobile, and power conservation for these battery-operated devices is important. Two modes of operation are provided to reduce battery drain.

An AMS in sleep mode remains in the connected state but has pre-negotiated periods of absence. A series of alternate listening and sleep windows are available, and these can be dynamically switched between sixteen patterns available (only three modes are available with the legacy system). During an AMS's listening window, the ABS can transmit traffic indication messages to indicate the presence of traffic due for the AMS. If there is no traffic due, the AMS reverts to sleep mode for the rest of the listening window, saving more power.

An AMS in Idle state is only available periodically for DL broadcast traffic messaging without registering at an ABS. This allows further reduction in power and radio resources. An idle AMS wakes at paging intervals and monitors paging broadcast messages sent by the ABS. An AMS can terminate the idle state and transit into the access state to perform network-reentry procedures with ABS.

8. Scheduling Services

The scheduler takes into consideration the bandwidth request, QoS associated with the service flow, and channel conditions of the MSs to allocate radio resources (in terms of subcarriers and time within each OFDMA frame), to decide the modulation and coding scheme (MCS), and to determine the MIMO parameters used for individual service flows.

9. Bandwidth Request and Allocation

Transmission bandwidth is centrally controlled by the ABS, and the AMS needs to signal the ABS to request bandwidth to adjust to traffic conditions. It has several means to do this [15] (Section 16.2.11.1). Firstly, a contention-based random access bandwidth request can be used. The MS can do this by transmitting a bandwidth request pre-amble sequence and a quick-access message (12 bits) on the bandwidth request channel. This process is illustrated in Figure 9. Secondly, a standalone bandwidth request header can be used by the AMS to send a bandwidth request in step three of the "five-step, contention-based random access BR" procedure or as a response to the polling from ABS.

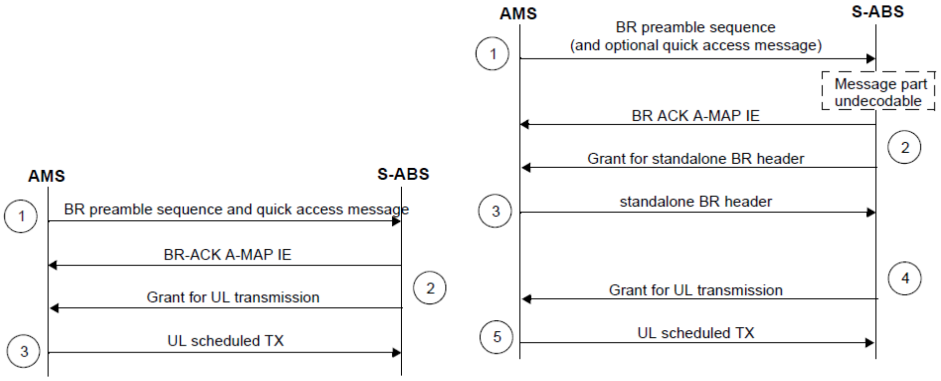

AMS
S-ABS
1
BR preamble sequence and quick access message
BR-ACK A-MAP IE
2
Grant for UL transmission
3
UL scheduled TX
AMS
S-ABS
1
BR preamble sequence
(and optional quick access message)
Message part undecodable
BR ACK A-MAP IE
2
Grant for standalone BR header
3
standalone BR header
4
Grant for UL transmission
5
UL scheduled TX

Figure 9. Contention-based bandwidth request (three step and five step) (From [15] section 16.2.11.1.1).

Thirdly, piggybacked bandwidth request can be used by an AMS to request bandwidth for the same or a different connection by attaching an extender header to a MAC PDU carrying a data payload. Fourthly, bandwidth request can also be done through primary fast-feedback channel (P-FBCH) in one of the two ways. The first way involves utilizing the bandwidth request indication flag feedback. An AMS can send a specific codeword (representing a BR indication flag) on the P-FBCH to indicate to the ABS its intention to request UL allocation, without the need to perform a random access bandwidth request.

The second way is termed the extended real-time packet service (ErtPS)/ adaptive granting and polling (aGP) service bandwidth request. By sending a specific codeword through P-FBCH, the AMS can inform the ABS of pending ertPS data.

10. Automatic Repeat Request (ARQ)/Hybrid Automatic Repeat Request (HARQ)

ARQ and HARQ are schemes for error control. An ARQ block can be generated from one or more MAC service data units (SDUs) or MAC SDU fragment(s). ARQ blocks are sequentially numbered and can vary in size. ARQ and HARQ can be applied on a flow at the same time. Should the HARQ checks fail, the HARQ entity can inform the ARQ entity to trigger retransmission and re-segmentation of ARQ blocks. For the downlink, IEEE 802.16m uses adaptive synchronous HARQ, where resource allocation and transmission format for retransmission may vary from that of the original transmission, and control signals are needed to indicate changes. For uplink, a non-adaptive synchronous HARQ scheme is used, meaning that the parameters and resource allocation for the retransmission are known in advance. An illustration of HARQ operation in TDD mode for DL and UL [14] is provided in Figure 10.

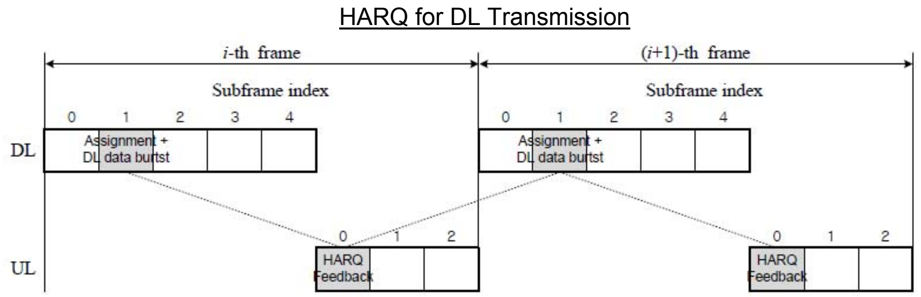


Figure 10. Example of TDD DL and UL HARQ timings (From [14]) (continued on next page)

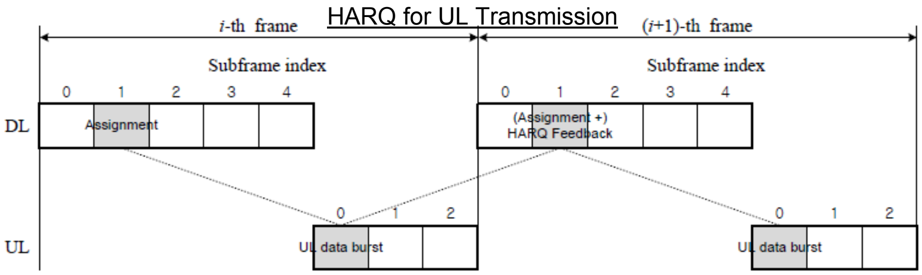


Figure 10 (contintued from previous page).

11. Security Sublayer

The diagram in Figure 11 provides an overview of IEEE 802.16m security architecture. Entities can be grouped into two categories: security management or encryption and integrity. The latter consists of a user data encryption and authentication entity and a management message authentication/confidentiality entity, as well as an authentication entity for standalone signaling headers.

The advanced encryption standard (AES) counter mode with cipher block chaining message authentication code (CCM), often referred to as AES-CCM, is a symmetrical block cipher supported by IEEE 802.16m, providing authentication and privacy. The encryption and integrity entities rely on AES-CCM to provide confidentiality and integrity functions under the control of the security management entities.

Security management entities consist of overall security management and control entity, authentication and security association (SA) control entity, privacy key management (PKM3) entity, extensible authentication protocol (EAP) entity, and location privacy entity.

The overall security management and control entity manages and coordinates the operation of the other security entities. The authentication and SA control entity manages the formation of security associations. The SA contains information related to a connection, such as the level of security applied or UL and DL traffic encryption keys (if applicable). Some of these are dependent on the outcome of capability negotiation, where ABS and AMS agree on the level of security to adopt. The PKM3 entity is responsible for performing mutual and unilateral authentication and establishes confidentiality between the ABS and AMS through a series of steps and algorithms that ensure secure key exchange through an unsecure connection. The EAP encapsulation/de-encapsulation entity is responsible for exchanging EAP messages as part of PKM3 to perform authentication and authorization functions.

The last entity is the location privacy entity. IEEE 802.16-2009 does not provide means of concealing the identity of AMS. A real MAC address is used during initial ranging and registration during network entry, and the connection IDs (CIDs) issued in plain can be used to identify and track an MS throughout the whole session. IEEE 802.16m provides the means to use a pseudo identity during network entry, and the station ID (STID) used to address AMSs is issued under protection of encryption.

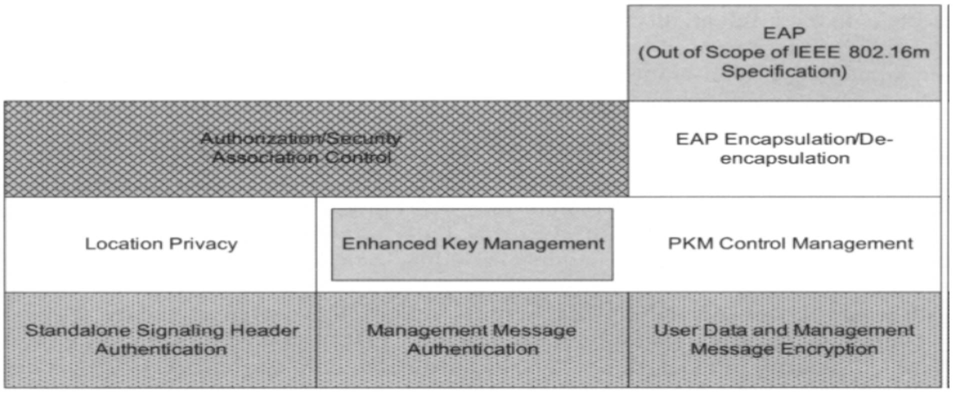


Figure 11. Functional blocks within 802.16m security architecture (From [14]).

C. PHYSICAL LAYER

1. Orthogonal Frequency-Division Multiple Access

Orthogonal frequency-division multiplexing (OFDM) is a form of multi-carrier modulation technique that distributes data across multiple carriers. These carriers’ frequencies are selected such that adjacent subcarriers are separated by the subcarrier symbol rate, therefore, maintaining spectral orthogonality. This essentially enables high data throughput while limiting the effects of inter-symbol-interference (ISI) and multipath distortion, since OFDM symbol duration is made much longer than is the case without multiple carriers. In addition, a cyclically extended guard interval, where each OFDM symbol is prefixed with a periodic extension of the signal itself, can be added, called a cyclic prefix (CP). Thus, when this guard interval is longer than multipath delay, the ISI can be effectively eliminated [14]. To support multiple users, the whole OFDM channel can be time-multiplexed among different users. This process is illustrated in Figure 12.

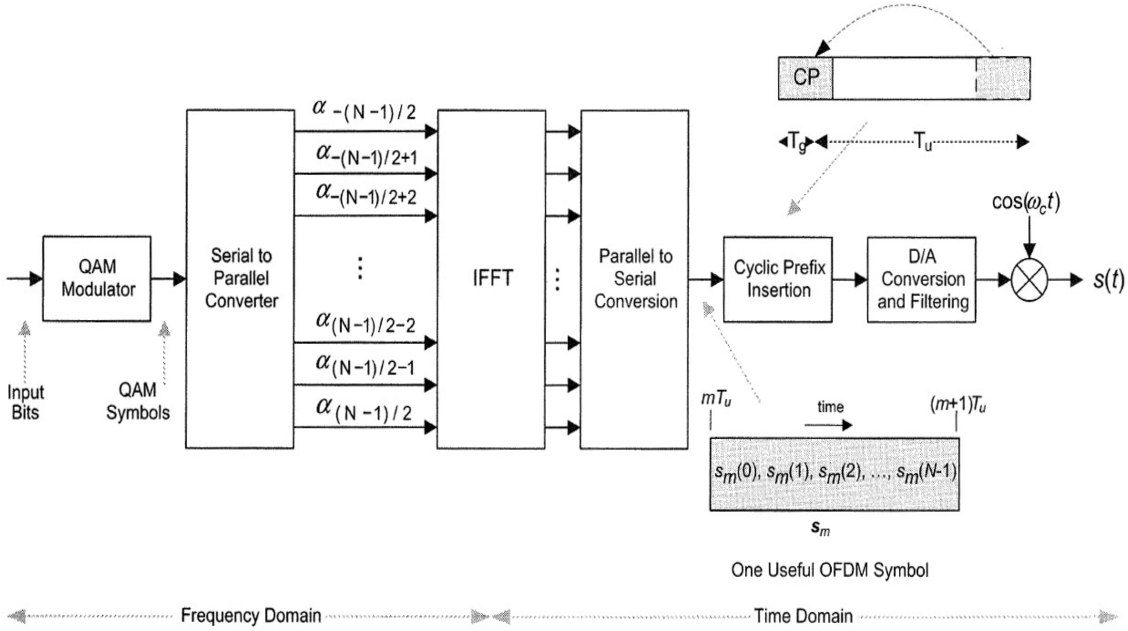


Figure 12. OFDM generation and cyclic prefix (From [14]).

Orthogonal frequency-division multiple access (OFDMA) takes the time multiplexed OFDM concept one step further by simultaneously multiplexing across the frequency domain (see Figure 13). This is done by allowing the assignment of subcarriers to different users over time. Hence, radio resources can be divided in a granular manner into resource blocks and assigned to users dynamically, on the fly, by a scheduler. The scheduler can take channel conditions and the QoS of the service flow into consideration and, among other factors, optimize every frame in a manner that is responsive to demand. OFDMA is available for use in IEEE 802.16 for both UL and DL.

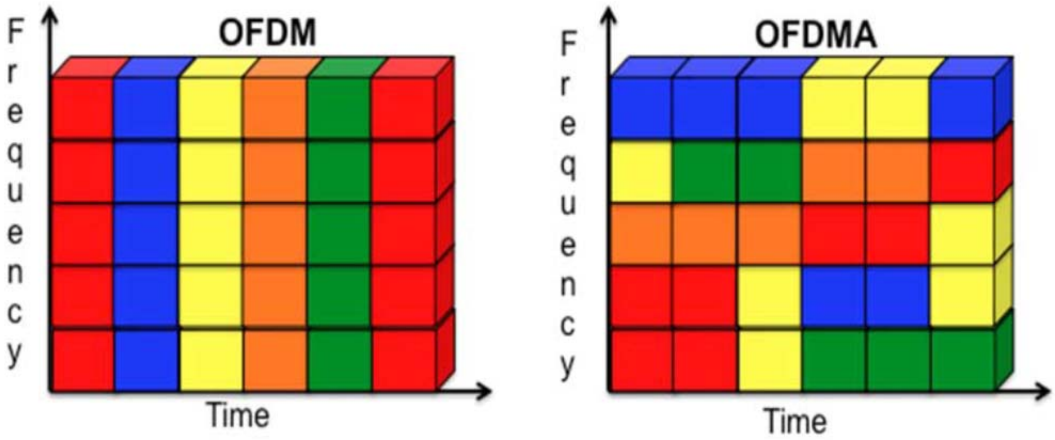


Figure 13. Conceptual comparison between OFDM and OFDMA (From [16]).

2. Frame Structure

The IEEE 802.16m frame is illustrated in Figure 14. A super frame consists of four frames lasting 5 ms each. Within each frame are subframes with transmit/receive switching intervals included. Each subframe consists of a number of OFDM symbols with CP before each symbol. How the system parameters can change with different data bandwidths selected is shown in Table 2.

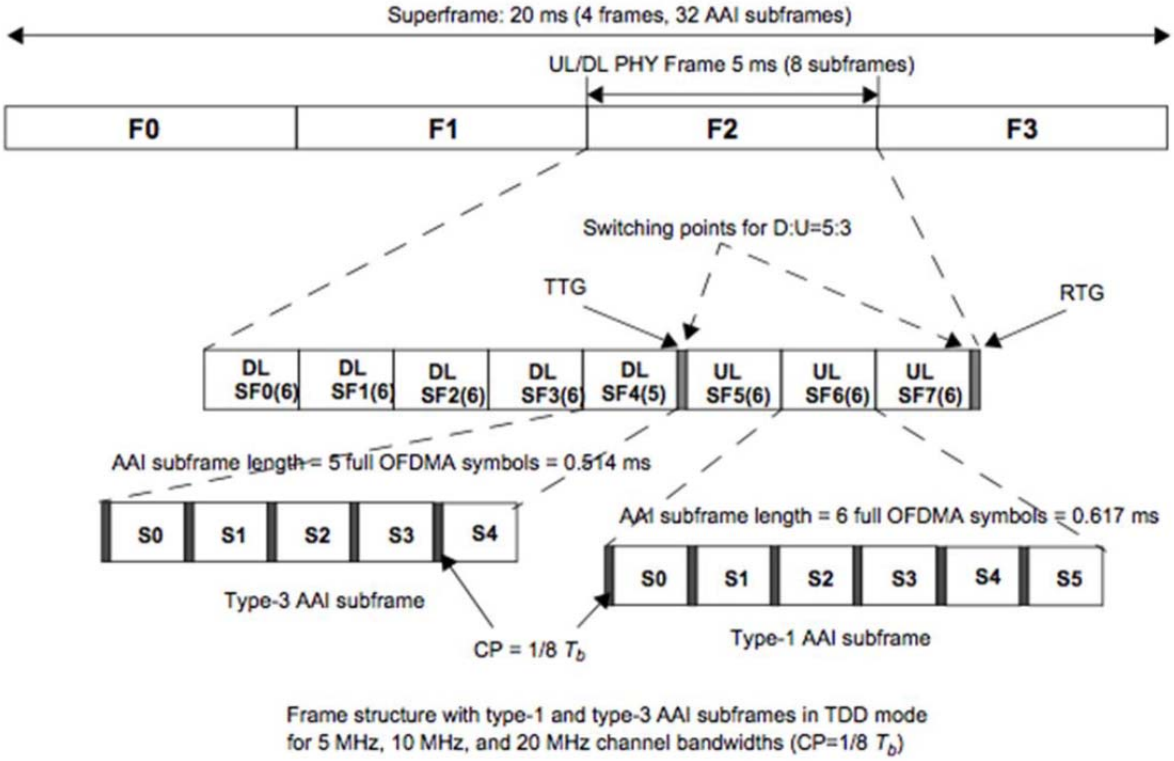
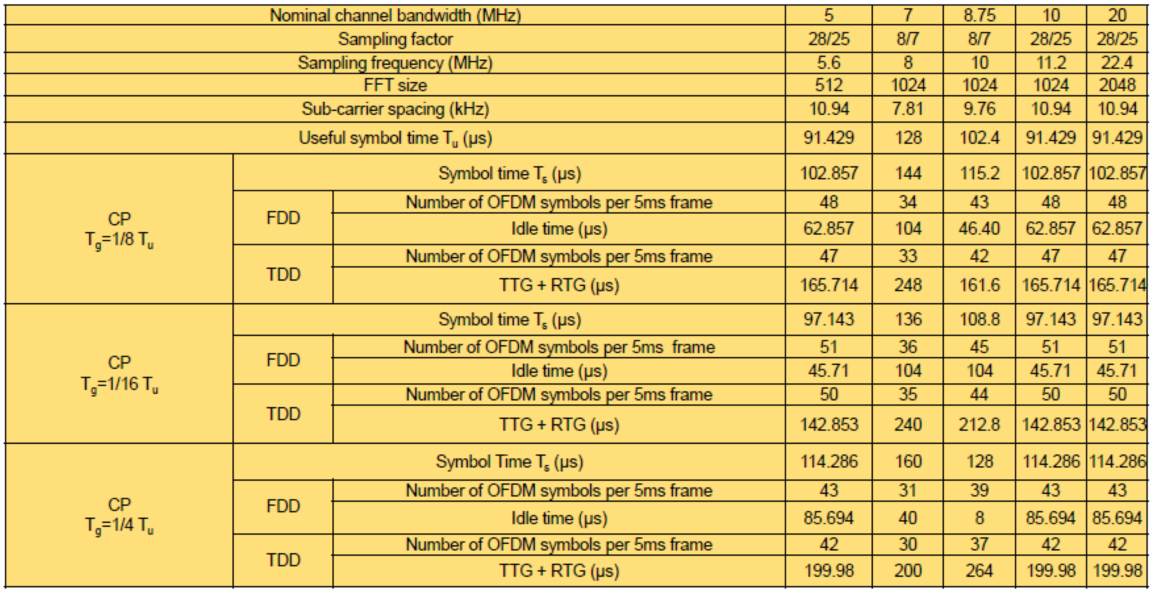

Superframe: 20 ms (4 frames, 32 AAI subframes)
UL/DL PHY Frame 5 ms (8 subframes)
F0
F1
F2
F3
Switching points for D:U=5:3
TTG
RTG
DL SF0(6)
DL SF1(6)
DL SF2(6)
DL SF3(6)
DL SF4(5)
UL SF5(6)
UL SF6(6)
UL SF7(6)
AAI subframe length = 5 full OFDMA symbols = 0.514 ms
S0
S1
S2
S3
S4
Type-3 AAI subframe
AAI subframe length = 6 full OFDMA symbols = 0.617 ms
S0
S1
S2
S3
S4
S5
Type-1 AAI subframe
CP = 1/8 T_b
Frame structure with type-1 and type-3 AAI subframes in TDD mode
for 5 MHz, 10 MHz, and 20 MHz channel bandwidths (CP=1/8 T_b)

Figure 14. Frame structure illustration for TDD and CP=1/8 (From [15] section 16.3.3.2.2).

Table 2. Frame timings with different bandwidths and CP (From [15]).



Nominal channel bandwidth (MHz)			5	7	8.75	10	20
Sampling factor			28/25	8/7	8/7	28/25	28/25
Sampling frequency (MHz)			5.6	8	10	11.2	22.4
FFT size			512	1024	1024	1024	2048
Sub-carrier spacing (kHz)			10.94	7.81	9.76	10.94	10.94
Useful symbol time T_u (μs)			91.429	128	102.4	91.429	91.429
CP T_g=1/8 T_u	Symbol time T_s (μs)		102.857	144	115.2	102.857	102.857
	FDD	Number of OFDM symbols per 5ms frame	48	34	43	48	48
		Idle time (μs)	62.857	104	46.40	62.857	62.857
	TDD	Number of OFDM symbols per 5ms frame	47	33	42	47	47
		TTG + RTG (μs)	165.714	248	161.6	165.714	165.714
CP T_g=1/16 T_u	Symbol time T_s (μs)		97.143	136	108.8	97.143	97.143
	FDD	Number of OFDM symbols per 5ms frame	51	36	45	51	51
		Idle time (μs)	45.71	104	104	45.71	45.71
	TDD	Number of OFDM symbols per 5ms frame	50	35	44	50	50
		TTG + RTG (μs)	142.853	240	212.8	142.853	142.853
CP T_g=1/4 T_u	Symbol Time T_s (μs)		114.286	160	128	114.286	114.286
	FDD	Number of OFDM symbols per 5ms frame	43	31	39	43	43
		Idle time (μs)	85.694	40	8	85.694	85.694
	TDD	Number of OFDM symbols per 5ms frame	42	30	37	42	42
		TTG + RTG (μs)	199.98	200	264	199.98	199.98

3. Subchannelization

Available physical OFDM subcarriers and OFDM symbols are grouped into physical resource units (PRUs), and these are remapped into two types of logical entities: contiguous resource units (CRUs) and distributed resource units (DRUs). Partitioning frequencies in this manner facilitates fractional frequency reuse (FFR). CRUs are optimized for frequency scheduling gain, while DRUs are good for frequency diversity gain [14]. The mapping process is illustrated in Figure 15, which shows how PRUs are grouped into CRUs and DRUs and mapped into Logical Resource Units (LRUs).

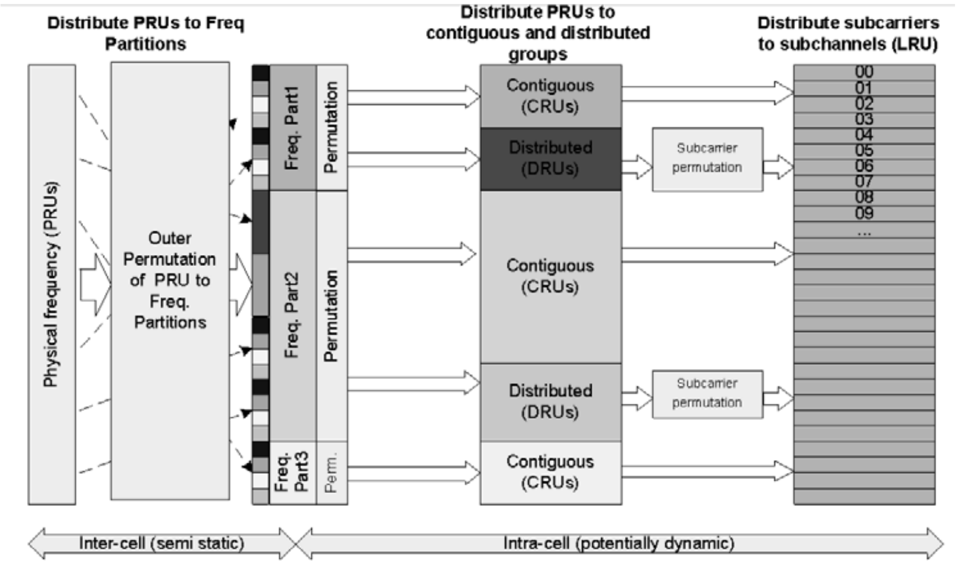


Figure 15. Physical to logical mapping process (From [14]).

4. Channel Coding and Modulation

The role of channel coding is to introduce redundancy into the data transmitted to enable correction of bit errors at the receiver end without further intervention from the transmitter. The net effect is to decrease the error rate, reduce transmission power, and increase transmission distance [14]. For data channels, IEEE 802.16m uses convolutional turbo code (CTC) with a minimum code rate of 1/3. The coding and modulation process for traffic channels is summarized in Figure 16. For control channels, a tail-biting convolutional code (TBCC) with minimum rate of ¼ is used for control channels. This form of coding is slower but more reliable. For HARQ feedback channels, HARQ incremental redundancy coding is used, while different versions of constellation rearrangement (CoRe) are used for 16QAM and 64QAM data.

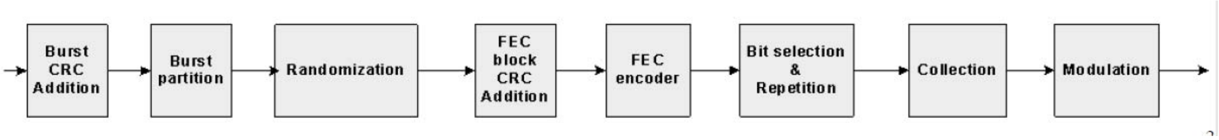


Figure 16. Coding and modulation process (From [17]).

Note that all data is randomized or scrambled as part of the coding and modulation process using a pseudo-random binary sequence (PRBS) generated by the circuit shown in Figure 17. This operation is performed on all data except the frame control header (FCH) and preambles, and the generator is reinitialized with a fixed sequence [LSB] 0 1 1 0 1 1 1 0 0 0 1 0 1 0 1 [MSB] for every forward error correction (FEC) block. Since the sequence is known and fixed, the scrambled data transmitted over the air can be decoded into plain data, and plain data can be encoded into scrambled data for transmission. For the purpose of this thesis, underlying plain data scrambled with this process is regarded as available, and scrambled data can be generated from any plain data desired.

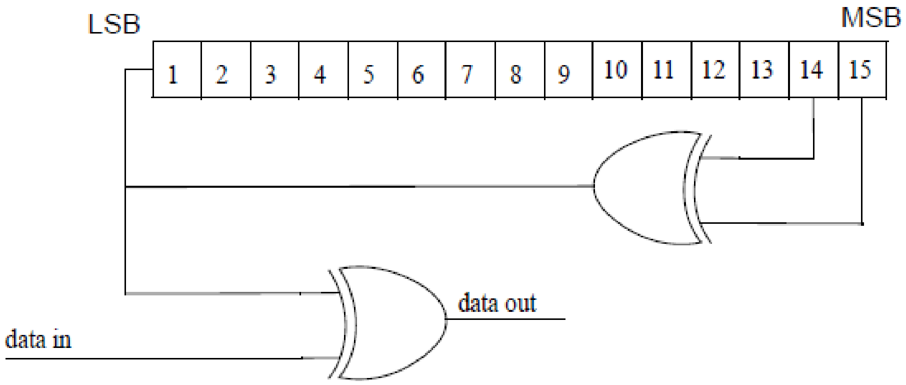


Figure 17. PRBS generator (From [15] section 16.3.10.1.3).

5. Synchronization Channel

The first step in network entry involves discovery, which is followed by timing and frequency acquisition, DL synchronization, and base-station identification. The primary advanced preamble (PA-Preamble) and secondary advanced preamble (SA-Preamble) within IEEE 802.16m provides a two-stage process to accomplish these. The PA-Preamble is located at the first OFDMA symbol within the second frame of the superframe. This narrowband synchronization signal is used for initial acquisition, synchronization, and broadcast of system information including the system bandwidth. The SA-Preamble is located at the first OFDMA symbol within the first and third frames of a superframe. This wideband preamble is responsible for fine synchronization and cell/sector identification (Cell ID).

The location of the advanced preambles is illustrated in Figure 18.

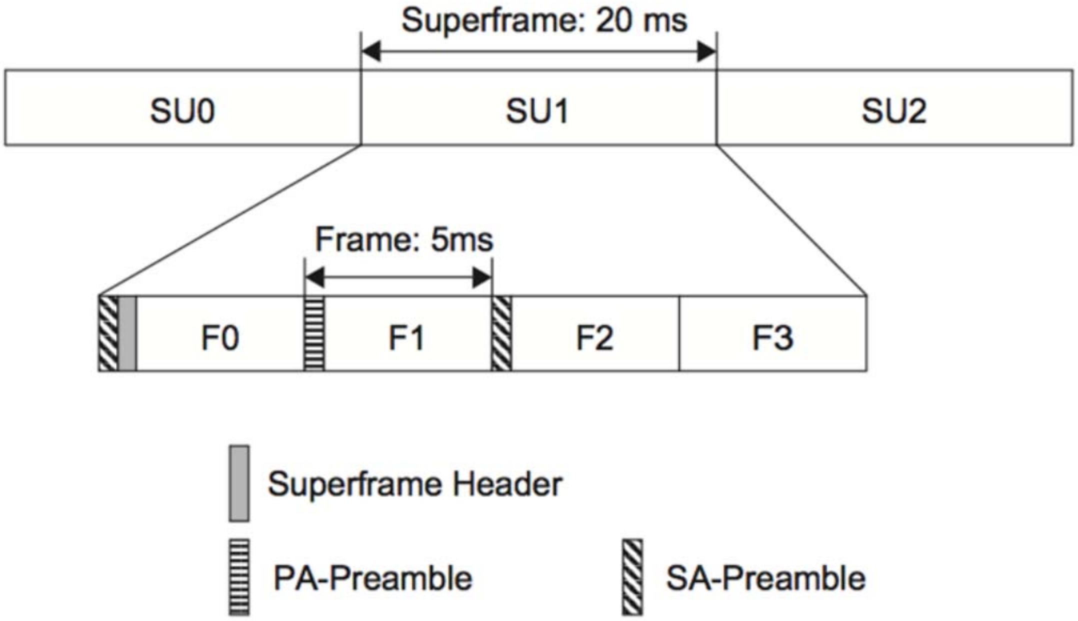


Figure 18. Location of preambles (From [11]).

6. Superframe Headers (Part of Broadcast Channel)

After achieving synchronization and obtaining key system parameters from the advanced preambles, the superframe header contains the next batch of information essential for network entry, reentry, and communication maintenance. The superframe header is located in the first subframe of every superframe, occupying the second to the sixth OFDMA symbol of the subframe. The location of the SFH is illustrated in Figure 19. The primary superframe header (P-SFH) occupies the first few data logical-resource units (DLRU) within the SFH, and it is transmitted with fixed MCS: quadrature phase-shift keying (QPSK) with TBCC coding at 1/24 effective code rate. The secondary superframe header (S-SFH) occupies DLRUs after P-SFH, and it can be divided into three subtypes: sub-packet 1 with network reentry information, sub-packet 2 with initial entry information, and sub-packet 3 with remaining system information. Transmission of S-SFH1, S-SFH2, and S-SFH3 are interspersed over several superframes; an example of this configuration is illustrated in Figure 20.

Physical processing of SFH is illustrated in Figure 21.

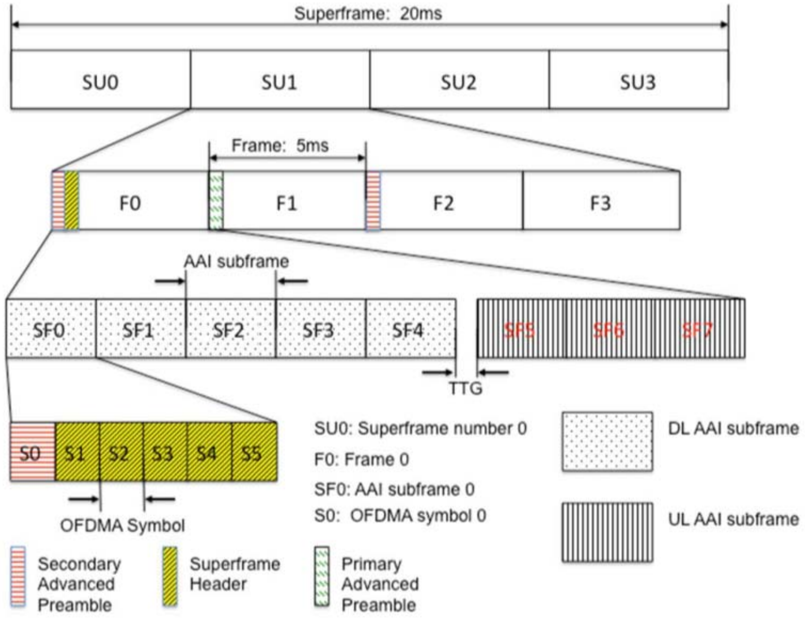


Figure 19. Positioning of superframe header within superframe (From [15]).

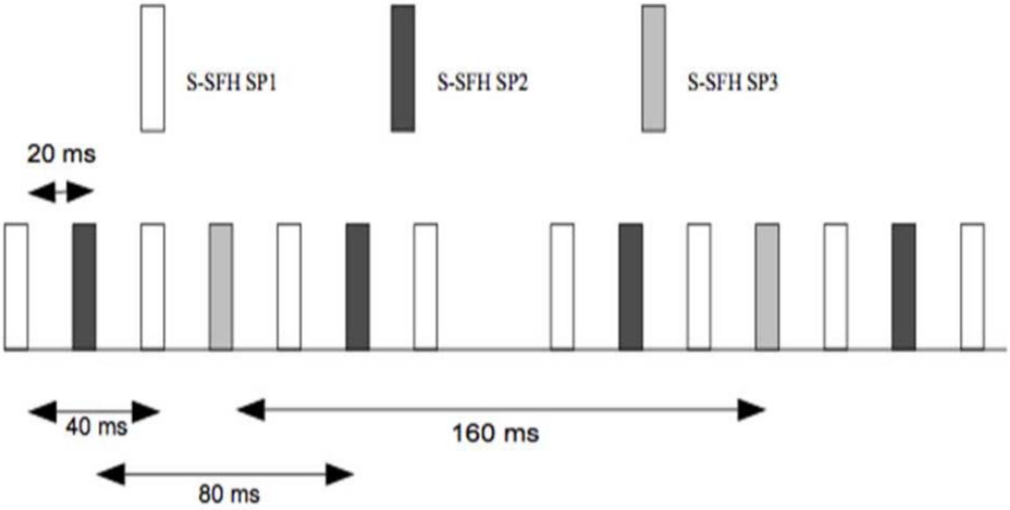


Figure 20. Illustration of secondary superframe header position across superframes (From [15]).

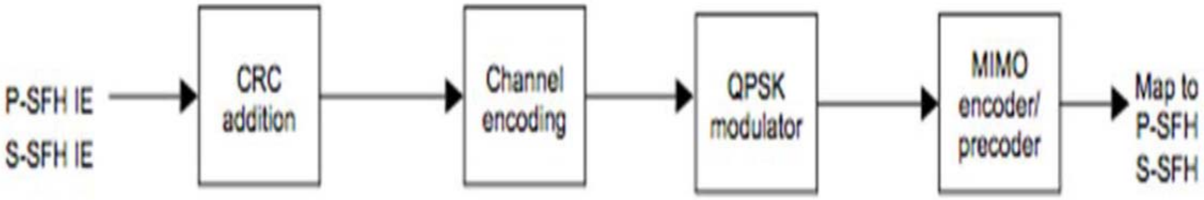


Figure 21. Processing for superframe headers (From [15] section 16.3.5.3.1.1).

7. Downlink Control Channels

There are two forms of downlink control: MAC control/management messages as discussed in earlier sections and medium access protocol (MAP). Within legacy frames, MAPs were broadcast messages that were time-division multiplexed with data and jointly encoded for use by all MSs. Their main purpose is to inform all users on radio resource allocation for the entire frame. Although the legacy MAPs are scrambled, the algorithm and its start states are known, and, for the purpose of this thesis, available to an attacker. Hence, the commonly decodable DL and UL MAPs enable all MSs to know exactly which subcarriers and OFDMA symbols they are assigned for uplink and downlink. An illustration of legacy MAPs within context of a frame is provided in Figure 22.

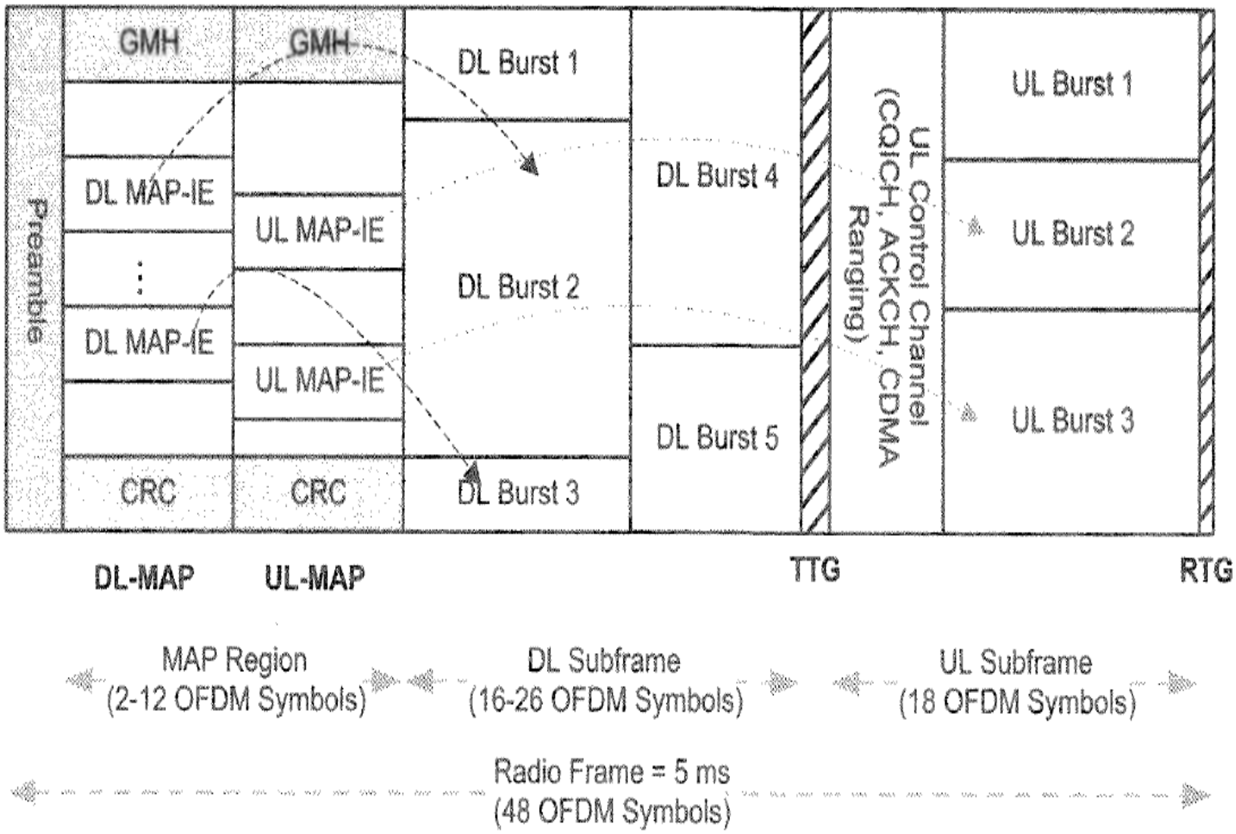

Preamble
GMH
GMH
DL MAP-IE
:
DL MAP-IE
UL MAP-IE
UL MAP-IE
CRC
CRC
DL Burst 1
DL Burst 2
DL Burst 3
DL Burst 4
DL Burst 5
UL Control Channel (CQICH, ACKCH, CDMA Ranging)
UL Burst 1
UL Burst 2
UL Burst 3
DL-MAP
UL-MAP
TTG
RTG
MAP Region (2-12 OFDM Symbols)
DL Subframe (16-26 OFDM Symbols)
UL Subframe (18 OFDM Symbols)
Radio Frame = 5 ms (48 OFDM Symbols)

Figure 22. Structure of legacy MAPs (After [14]).

Within IEEE 802.16m, key changes include the fact that it is now frequency multiplexed rather than time multiplexed and that control data for AMSs use different MCS to suit channel conditions experienced by individual AMSs. The overheads located within the A-MAP, in the context of the IEEE 802.16m frame, is illustrated in Figure 23.

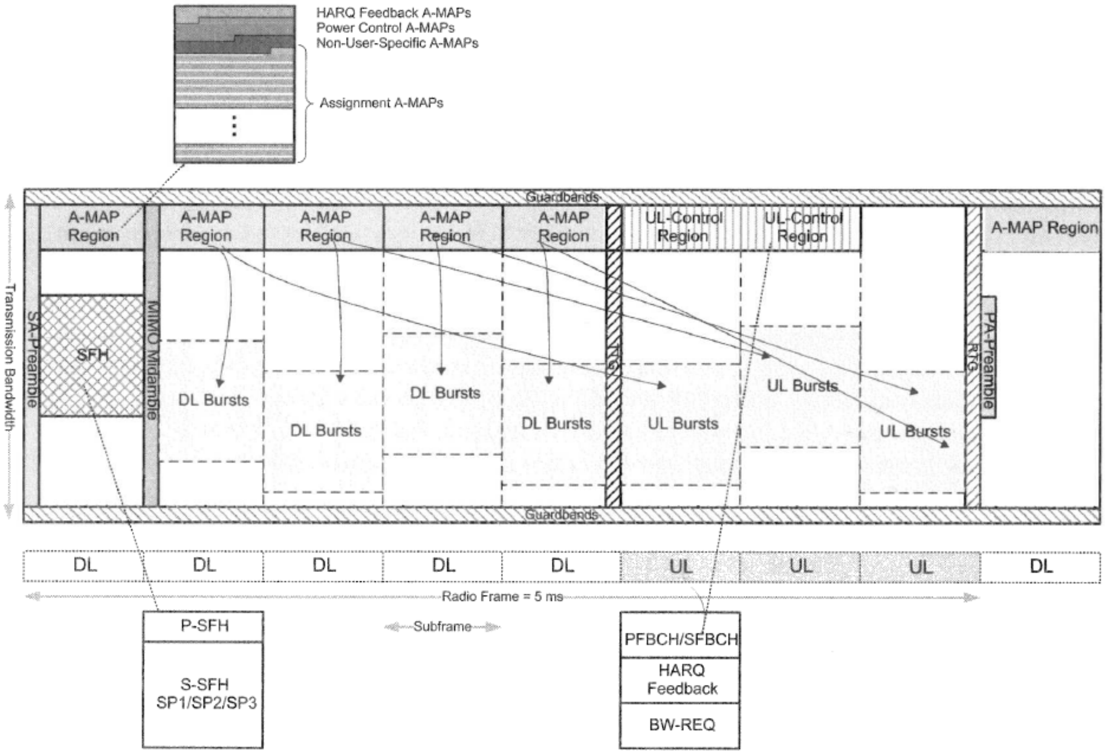


Figure 23. Structure of IEEE 802.16m overhead channels (From [14]).

The internal structure of DL A-MAP is illustrated in Figure 24. There are four different types of DL A-MAP: non-user-specific A-MAP, assignment A-MAP, HARQ feedback A-MAP, and power control A-MAP. The non-user-specific A-MAP contains common information for all AMSs, including parameters required to decode other control channels. The assignment A-MAP contains information on radio-resource assignment for broadcast, multicast and unicast communications for each individual AMS. Broadcast A-MAP information elements (IEs) are located at the beginning of either assignment A-MAP group 1 or 2 within the subframe. The HARQ feedback A-MAP contains feedback information for the hybrid automatic repeat request (HARQ). The power control A-MAP contains transmission power adjust values for each individual AMS, enabling ABS to quickly adjust AMS transmission power, albeit over a small range.

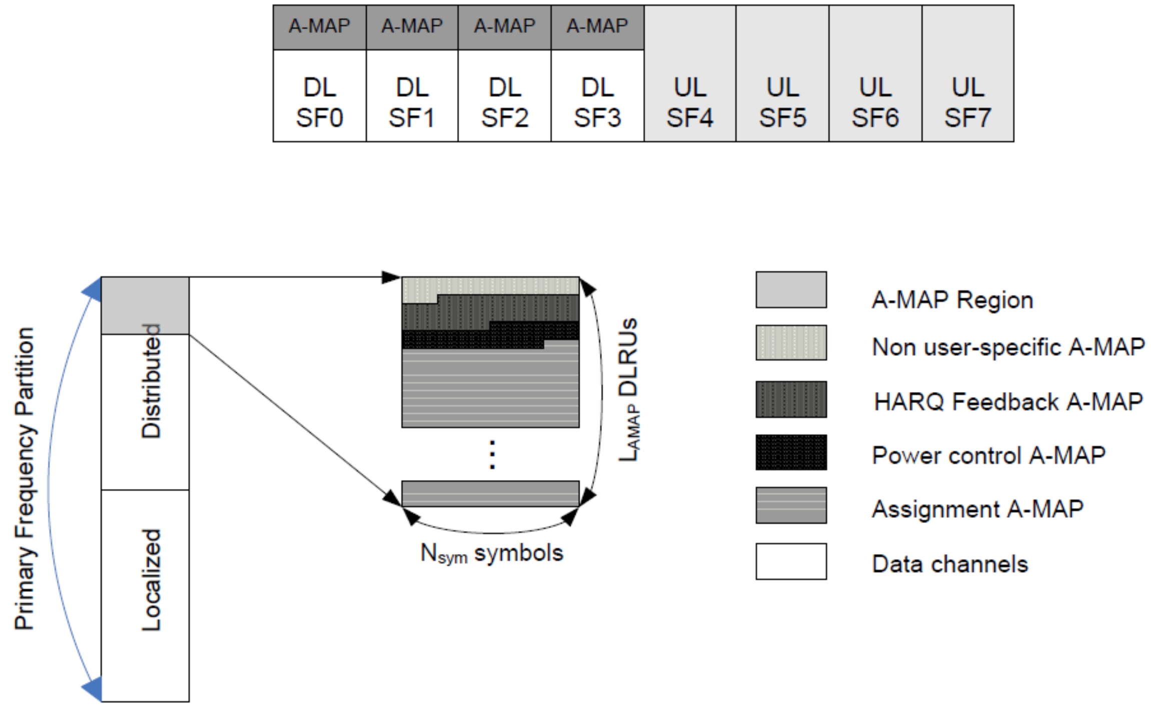


Figure 24. Structure of A-MAP region for IEEE 802.16m-2011 (From [14]).

The different channel coding processes for different A-MAPs [18] are depicted in Figure 25. Scrambling is performed for assignment A-MAPs (resource mapping) and HARQ data. Assignment A-MAPs information is first scrambled by a pseudo-random binary sequence (PRBS) generated by the circuit shown in Figure 26. If the assignment A-MAP is for unicast traffic, the random MAPMask-seed value is used to initialize the PRBS generator, and a CRC mask formed with the STID of the AMS is used to mask the A-MAP data ([15] section 16.3.5.3.2.4). The MAPmask seed and STID are transferred by the ABS to AMS in an encrypted manner after AMS registration during network entry. If the assignment A-MAP is for broadcast traffic, both the initialization vector and CRC mask are fixed values instead of random. The above is summarized in Table 3. The net outcome is that the attacker needs to overcome the obstacles put in place by the MAPMask seed as well as the STID in order to eavesdrop, or even target unicast traffic bursts, in IEEE 802.16m-2011. On the other hand, broadcast traffic in IEEE 802.16m-2011 remains as vulnerable as in legacy systems. It is also interesting to note that the HARQ feedback A-MAP is also scrambled, but only using STID, before coding and modulation.

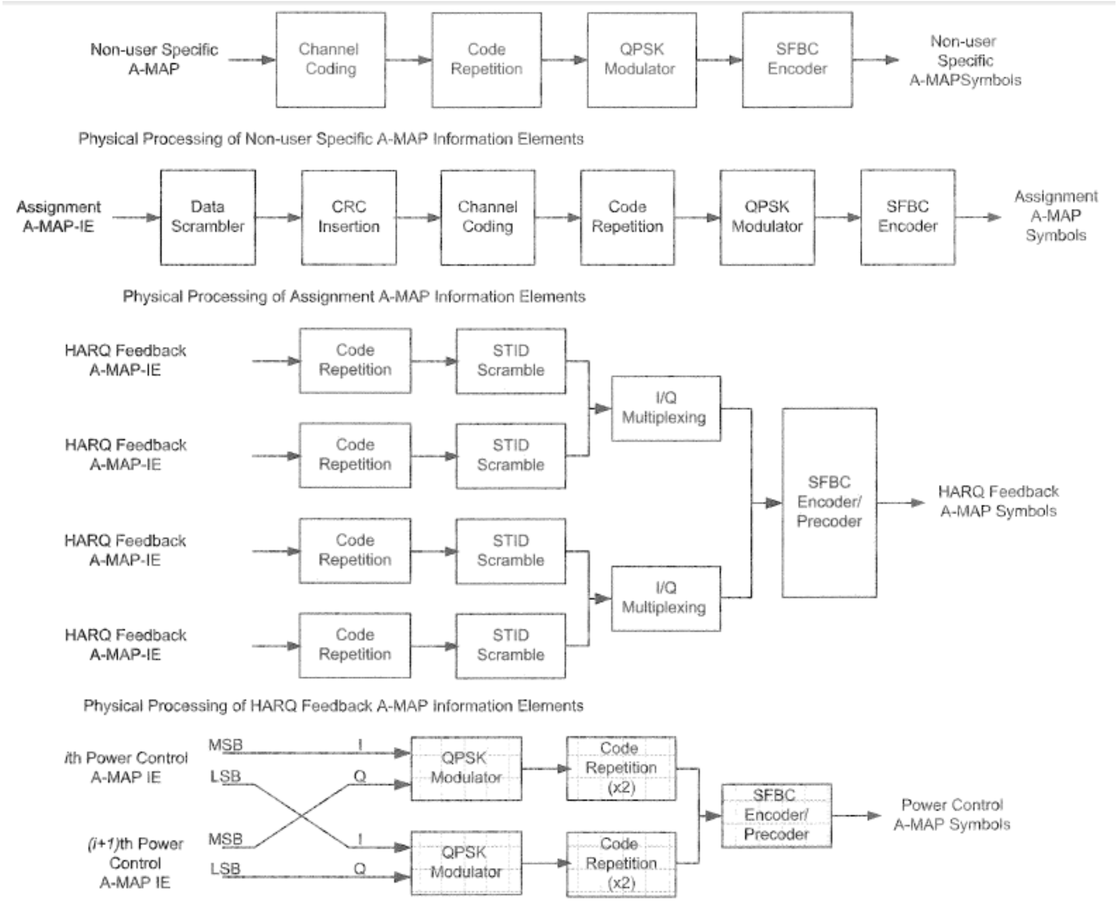


Figure 25. Physical layer procedures for A-MAPs in IEEE 802.16m-2011 (From [18]).

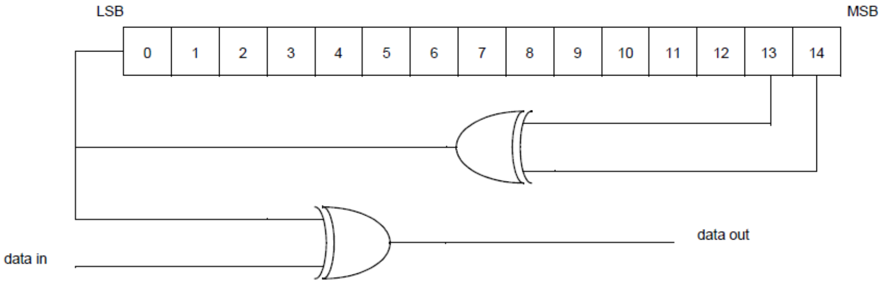


Figure 26. PRBS generator for scrambling assignment A-MAP in IEEE 802.16m-2011 (From [15] section 16.3.10.1.3).

Table 3. Initialization vector and CRC masks for assignment A-MAP scrambling in IEEE 802.16m-2011.

	Unicast	**Broadcast**
Initial Vector for PRBS Generator (15 bits)	"MAPMask Seed" Parameter Securely Passed to AMS during Network Entry	0b000100000000000
CRC Mask (16 bits)	0b0000 + 12 bit STID	0b0001000000000000

8. Uplink Control Channels

As previously seen in Figure 23, UL control channels are also frequency multiplexed. These UL control channels include the primary and secondary fast-feedback, HARQ feedback, sounding, ranging, and bandwidth request channels.

The primary and secondary fast-feedback channels carry different sets of channel quality as well as MIMO feedback. The primary fast-feedback channel carries wideband and narrowband channel quality indicators, while the secondary fast-feedback channel carries narrowband channel quality indicators. The structure and physical processing of these channels are illustrated in Figure 27. These feedback channels are frequency and time-division multiplexed in groups of feedback mini-tiles, and the secondary fast-feedback channels include pilots interspersed within them.

For the HARQ feedback channel, the ACK and NACK for DL transmissions occurring at predetermined intervals are transmitted on this channel using a combined TDM/FDM and TDM/CDM scheme. The structure of the HARQ feedback channel is illustrated in Figure 28. The channels are divided into HARQ mini-tiles (constructed by two subcarriers over two OFDM symbols), with each HARQ mini-tile identified by two indices, *m* and *k*. The *m* index is the HARQ mini-tile index within a HARQ feedback channel, and the *k* index is the HARQ feedback channel index.

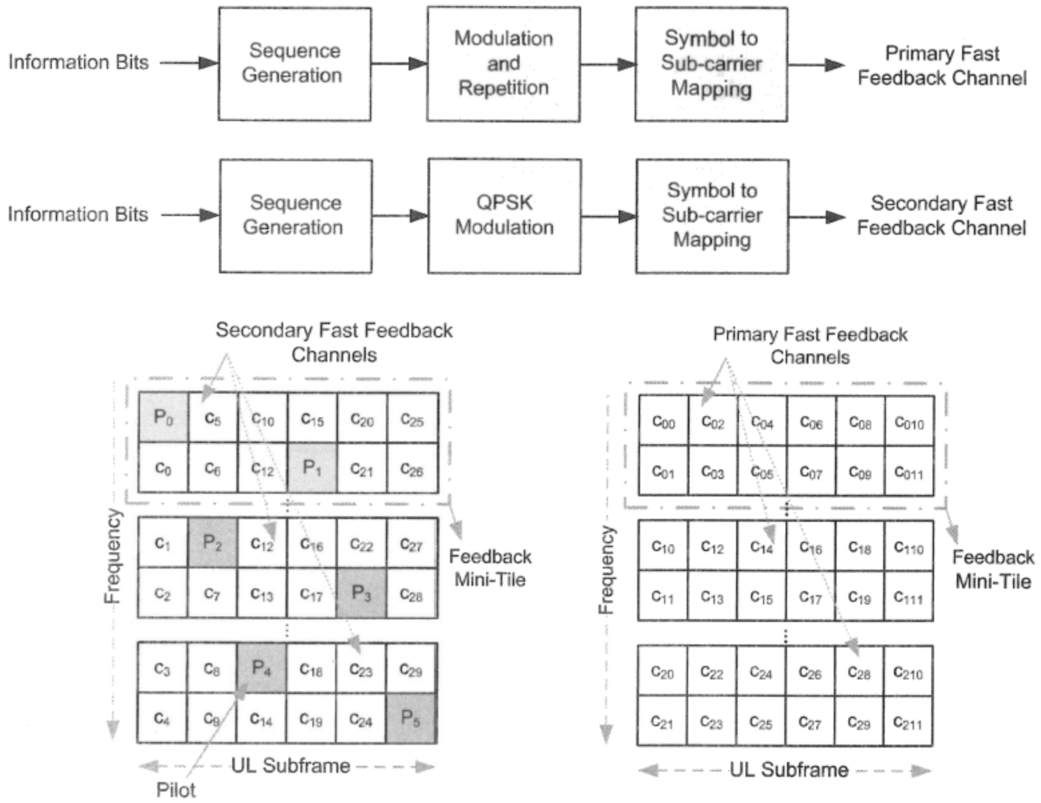


Figure 27. Physical processing and structure of primary and secondary feedback channels (From [18]).

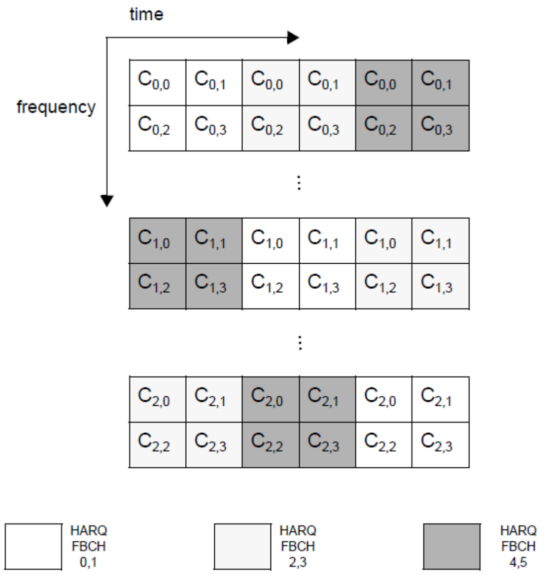

time
frequency
C0,0 C0,1 C0,0 C0,1 C0,0 C0,1
C0,2 C0,3 C0,2 C0,3 C0,2 C0,3
C1,0 C1,1 C1,0 C1,1 C1,0 C1,1
C1,2 C1,3 C1,2 C1,3 C1,2 C1,3
C2,0 C2,1 C2,0 C2,1 C2,0 C2,1
C2,2 C2,3 C2,2 C2,3 C2,2 C2,3
HARQ FBCH 0,1
HARQ FBCH 2,3
HARQ FBCH 4,5

Figure 28. Structure of HARQ mini tile (From [15]).

The sounding channel is used by the AMS to transmit sounding signals when instructed by the ABS, enabling measurements of the UL channel for MIMO and channel quality feedbacks at the ABS. The structure of the sounding channel is illustrated in Figure 29. The sounding channel is located in the second UL sub-frame and, depending on whether narrow-band or wideband channel is configured, the number of subcarriers used varies.

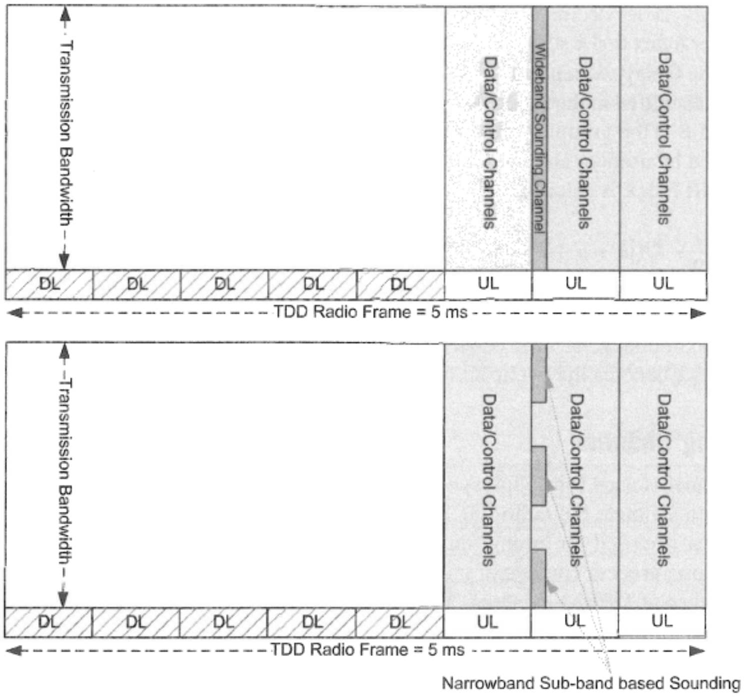


Figure 29. Structure of sounding channel in TDD mode (From [14]).

The ranging channel is used by the AMS to transmit ranging signals to initiate uplink synchronization. Upon receiving the incident signal, the ABS processes and computes important parameters such as power and frequency adjustments that will be feedback to the AMS. This allows the AMS to make adjustments, thereby attaining uplink synchronization and completing the initial ranging process. This initial ranging is contention based. Afterwards, the AMS can then proceed with network entry. For an AMS that has attained uplink synchronization, periodic (or synchronized) ranging needs to be performed continuously to maintain synchronization and is performed in a non-contention manner. Ranging signals typically consist of ranging preambles (RP) as well as cyclic prefixes (CP) appended before the RPs. Examples of ranging signals under different circumstances are shown in Figure 30.

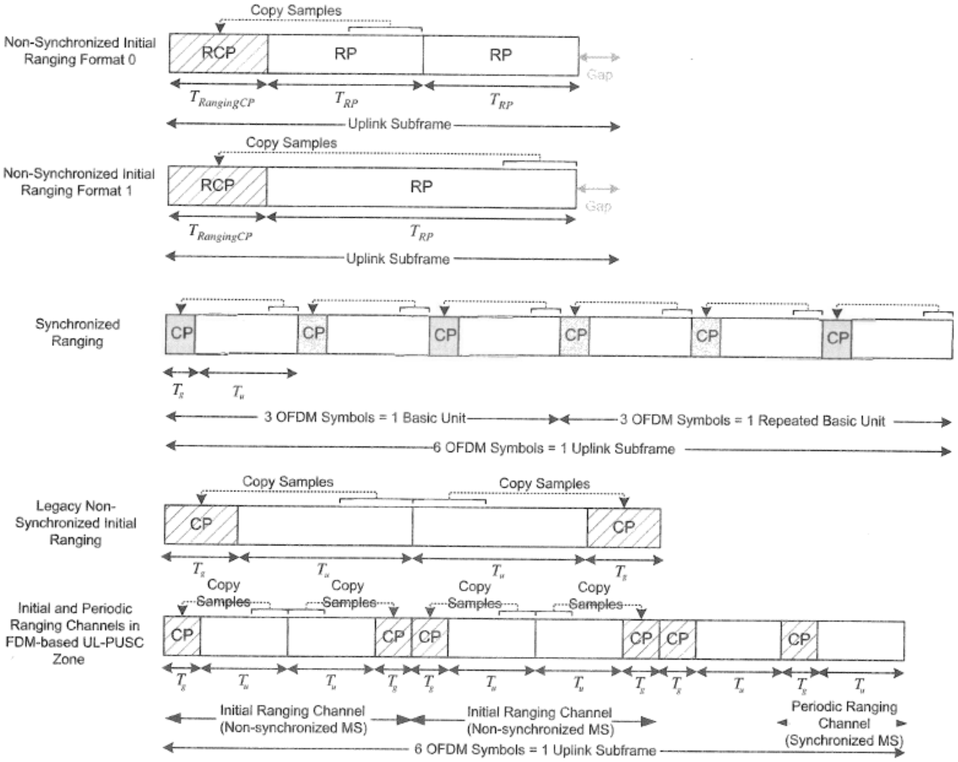

Copy Samples
Non-Synchronized Initial Ranging Format 0
RCP
RP
RP
Gap
$T_{RangingCP}$
T_{RP}
T_{RP}
Uplink Subframe
Copy Samples
Non-Synchronized Initial Ranging Format 1
RCP
RP
Gap
$T_{RangingCP}$
T_{RP}
Uplink Subframe
Synchronized Ranging
CP
CP
CP
CP
CP
CP
T_g
T_u
3 OFDM Symbols = 1 Basic Unit
3 OFDM Symbols = 1 Repeated Basic Unit
6 OFDM Symbols = 1 Uplink Subframe
Copy Samples
Copy Samples
Legacy Non-Synchronized Initial Ranging
CP
CP
T_g
T_u
T_u
T_g
Copy Samples
Copy Samples
Copy Samples
Copy Samples
Initial and Periodic Ranging Channels in FDM-based UL-PUSC Zone
CP
CP
CP
CP
CP
CP
T_g
T_u
T_u
T_g
T_g
T_u
T_u
T_g
T_g
T_u
T_g
T_u
Initial Ranging Channel (Non-synchronized MS)
Initial Ranging Channel (Non-synchronized MS)
Periodic Ranging Channel (Synchronized MS)
6 OFDM Symbols = 1 Uplink Subframe

Figure 30. Examples of ranging signals (From [18]).

As for bandwidth request channel, since all radio resources are managed centrally by the base station, any desired change in uplink parameters needs to be requested through the ABS. A contention based random access scheme is used by AMSs to request bandwidth. It involves a five-step or three-step quick-access procedure, illustrated in Figure 31. The physical channel structure for a bandwidth request channel is illustrated in Figure 32, subdivided into three UL tiles, where *Pr* denotes a preamble sequence. The quick-access message containing request information is QPSK modulated into 36 data symbols before being inserted into locations denoted by *M* within the three UL tiles (each containing 12 symbols) for transmission.

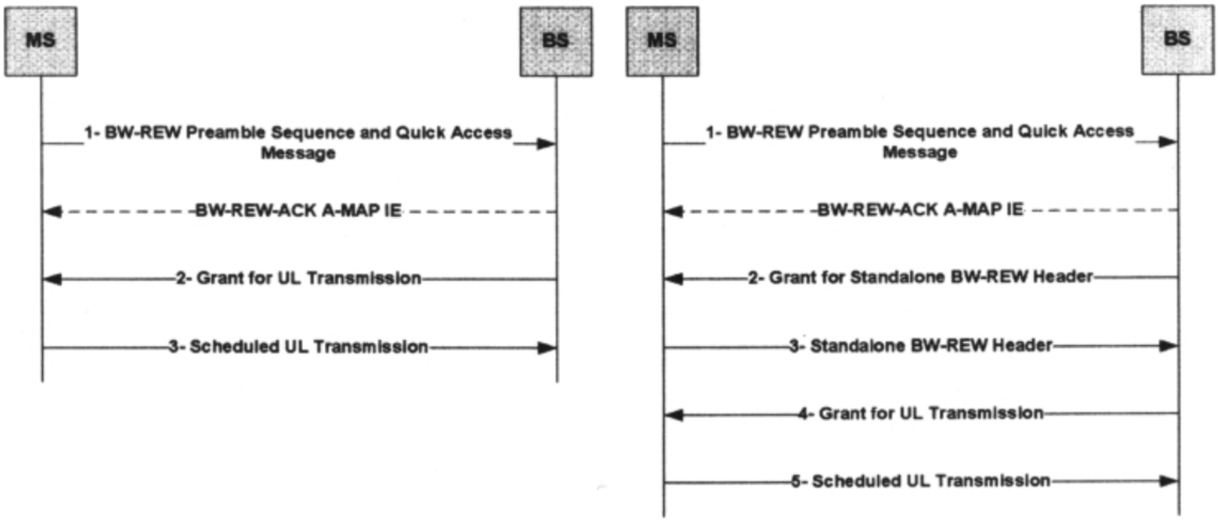
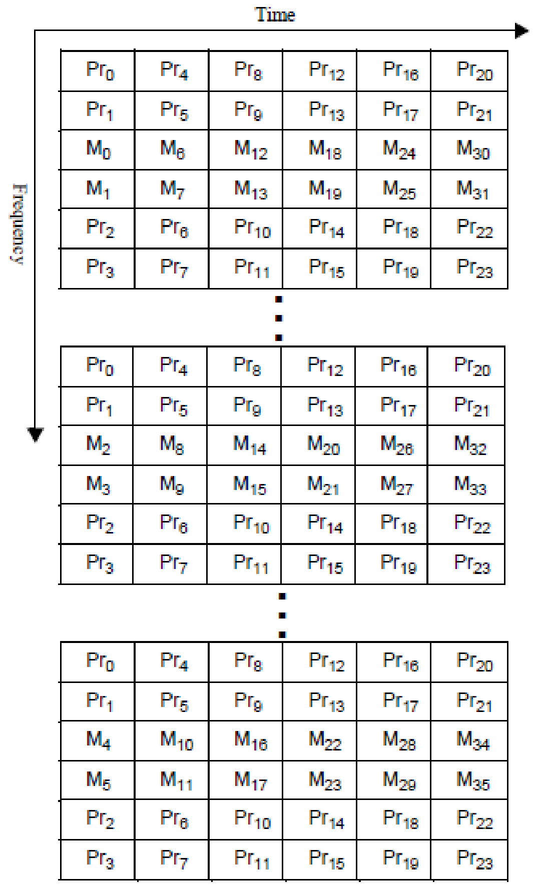

MS
BS
1- BW-REW Preamble Sequence and Quick Access Message
BW-REW-ACK A-MAP IE
2- Grant for UL Transmission
3- Scheduled UL Transmission
MS
BS
1- BW-REW Preamble Sequence and Quick Access Message
BW-REW-ACK A-MAP IE
2- Grant for Standalone BW-REW Header
3- Standalone BW-REW Header
4- Grant for UL Transmission
5- Scheduled UL Transmission

Figure 31. Bandwidth request procedures (From [14]).



Pr_0	Pr_4	Pr_8	Pr_{12}	Pr_{16}	Pr_{20}
Pr_1	Pr_5	Pr_9	Pr_{13}	Pr_{17}	Pr_{21}
M_0	M_6	M_{12}	M_{18}	M_{24}	M_{30}
M_1	M_7	M_{13}	M_{19}	M_{25}	M_{31}
Pr_2	Pr_6	Pr_{10}	Pr_{14}	Pr_{18}	Pr_{22}
Pr_3	Pr_7	Pr_{11}	Pr_{15}	Pr_{19}	Pr_{23}

Pr_0	Pr_4	Pr_8	Pr_{12}	Pr_{16}	Pr_{20}
Pr_1	Pr_5	Pr_9	Pr_{13}	Pr_{17}	Pr_{21}
M_2	M_8	M_{14}	M_{20}	M_{26}	M_{32}
M_3	M_9	M_{15}	M_{21}	M_{27}	M_{33}
Pr_2	Pr_6	Pr_{10}	Pr_{14}	Pr_{18}	Pr_{22}
Pr_3	Pr_7	Pr_{11}	Pr_{15}	Pr_{19}	Pr_{23}

Pr_0	Pr_4	Pr_8	Pr_{12}	Pr_{16}	Pr_{20}
Pr_1	Pr_5	Pr_9	Pr_{13}	Pr_{17}	Pr_{21}
M_4	M_{10}	M_{16}	M_{22}	M_{28}	M_{34}
M_5	M_{11}	M_{17}	M_{23}	M_{29}	M_{35}
Pr_2	Pr_6	Pr_{10}	Pr_{14}	Pr_{18}	Pr_{22}
Pr_3	Pr_7	Pr_{11}	Pr_{15}	Pr_{19}	Pr_{23}

Figure 32. Bandwidth request channel physical structure (From [15]).

9. Multiple Antenna Transmission Schemes

MIMO techniques are employed in IEEE 802.16m-2011 to achieve array gain, diversity gain, and spatial multiplexing gain to combat effects of multipath and channel spread.

a. DL MIMO

The wide range of MIMO modes available for downlink use can be broadly classified into single and multiple base-station modes.

A multi-base-station MIMO is an extension which entails AMSs being served by multiple ABSs through inter-BS coordination or even multi-BS transmission. For collaborative MIMO, several MSs are jointly served by multiple coordinated BSs, whereas in closed-loop macro diversity, every MS is served jointly by multiple coordinated BSs.

Single–user MIMO (SU-MIMO) techniques are point-to-point schemes that improve capacity and/or reliability through space-time/space-frequency codes together with spatial diversity multiplexing transmission. In single user (SU) schemes, one MS is addressed in one resource unit, while for multi-user (MU) schemes, multiple users can be scheduled in one resource unit.

Open-loop techniques are less reliant on channel information, including spatial multiplexing and space-time codes. These tend to result in a higher complexity burden at the receiver as well as less than optimal utilization of channel diversity or capacity. Closed-loop techniques make use of a feedback channel to relay channel information to the BS, enabling simpler techniques and better channel utilization [19].

A summary of how the preceding factors translate into actual MIMO modes is illustrated in Figure 33.

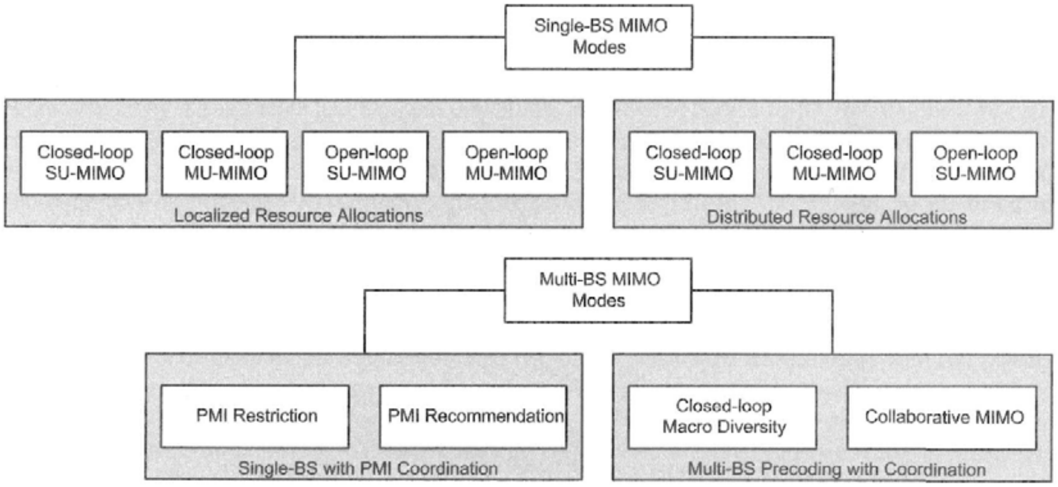


Figure 33. Summary of MIMO modes for DL (From [14]).

b. UL MIMO

MSs are constrained in terms of physical size and number of antennas. Hence, there are fewer options available for uplink MIMO. These MIMO modes include the open- and closed-loop versions of SU-MIMO and collaborative spatial multiplexing.

D. NETWORK ENTRY PROCESS

An AMS attempting network entry first commences downlink synchronization by means of the preambles and superframe headers before performing uplink synchronization through initial ranging. After ranging is complete, the ABS responds with an AAI-RNG-ACK message that contains power and timing adjust parameters to ensure uplink synchronization. It also issues a temporary station identifier (TSTID) along with a MAP mask seed and places them in the AAI-RNG-RSP message.

Capability negotiation messages are then exchanged before authentication, which involves the secure exchange of several sets of keys. Once this is done, selected MAC control messages and data messages being exchanged are encrypted and authenticated.

The AMS then requests registration through the AAI-REG-REQ message. Upon successful registration at the ABS, a response message, AAI-REG-RSP, is transmitted to the AM; the AAI-REG-RSP message conveys the real STID as well as the MAP mask seed. These two parameters, which are hidden from the casual observer, are instrumental in protecting the privacy of an AMS. They are used to scramble resource allocation mapping within assignment A-MAP control channels. The WiMAX network entry procedures are summarized in Figure 34.

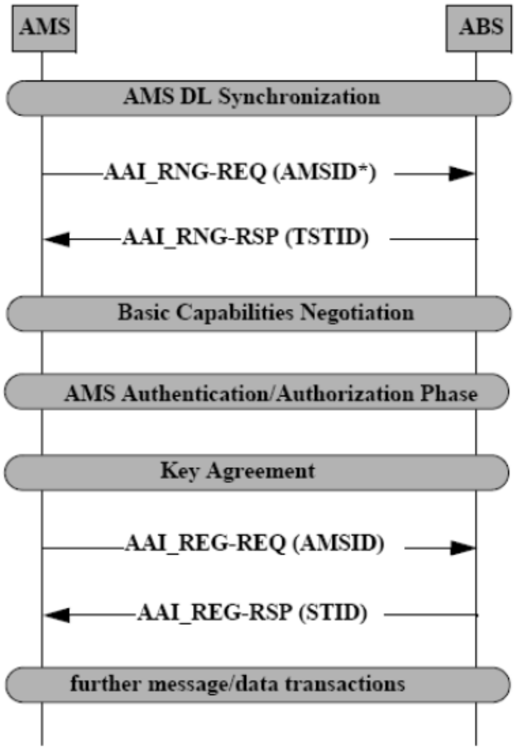


Figure 34. Network entry process (from [15] section 16.2.5.3.2)

III. SURVEY OF MAC CONTROL MESSAGES FOR VULNERABILITIES

A. BACKGROUND

MAC management messages are a key part of WiMAX control channels, and measures to protect these messages are examined in this chapter. An initial assessment is then performed to examine unprotected messages for weaknesses and to categorize them before examining selected examples in greater detail. This was performed for both legacy standards and IEEE 802.16m-2011.

B. PROTECTION MECHANISMS FOR MAC CONTROL MESSAGES

1. Integrity Check Value (ICV)

The ICV affords complete protection, including confidentiality, integrity and authenticity. This form of protection was first introduced with IEEE 802.16m-2011, and a majority of messages in that standard are protected in this manner compared with CMAC/HMAC, discussed below. In order for ICV to be used, security association needs to be established, which involves authentication as well as key exchange. This means that messages that normally receive protection do not during network entry prior to PKM negotiation. ICV protection is based upon the AES encryption scheme, which is currently regarded as secure and effective.

2. CMAC and HMAC

CMAC and HMAC provide protection for integrity and authenticity only. Although messages protected are still in plain, a hash generated from the encryption key is sent with the message and any attempt to alter contents results in the message failing authentication at the receiver. Even if the attacker attempts to replace the entire message, he would face the problem of generating a hash that can pass authentication procedures at the receiver, as he does not have the encryption key. Similar to ICV, protection requires security association to be completed. This means that messages that normally receive protection do not, prior to PKM negotiation.

C. CLASSIFICATION OF MAC MESSAGES BASED ON PROTECTION AND VULNERABILITIES

Based on the above criteria, the full list of MAC control messages for both IEEE 802.16m-2011 and IEEE 802.16-2009 were evaluated.

1. IEEE 802.16m-2011 MAC Management Messages

Out of 70 messages in total, 37 were fully protected by ICV. Nine were partially protected. Partial protection means that there are scenarios under which security association was not complete and MAC messages were not protected. The remaining 24 MAC messages were not protected. As the ICV protection is deemed effective, we regard messages under full ICV protection to be free from exploitation. A breakdown of the protection level for MAC management messages is provided in Table 4.

Table 4. Protection summary for IEEE 802.16m MAC control messages.

Total Number of Messages	70
Fully protected by ICV	37
Partial Protection	9
No Protection	24

For the MAC management messages that are not fully protected, the characteristics and workings of each message are examined in detail to ascertain possible exploitations. A summary of this assessment is provided in Table 5.

Table 5. Exploitation summary of IEEE 802.16m MAC control messages.

Total Messages Not Fully Protected	33
Limited Exploitation Scope	10
Messages With Possible Exploitation	23

As discussed earlier, due to the scrambling of assignment A-MAP by IEEE 802.16m, unicast messages cannot be exploited. Hence, remaining messages are further categorized according to attack nature and functional groups (see Table 6).

Table 6. Exploitation summary of IEEE 802.16m MAC control messages according to type and functional group.

General Message Modification Attacks	6
Power Related Message Modification Attacks	2
MIMO Related Message Modification Attacks	3
Flooding Attacks	2
Water Torture Attacks	2
Total Possible Exploitations	**15**

The details of the above exploits are discussed in the following subsections, with emphasis on selected categories of attacks. Most of the vulnerabilities identified involve injecting spoofed MAC control messages to the ABS or the AMS.

2. IEEE 802.16-2009 MAC Management Messages

A similar process is carried out for IEEE 802.16-2009. Out of 71 messages in total, nine are reserved, leaving 62 possible messages. Out of these 62, 30 are authenticated by CMAC/HMAC, leaving 32 that are both in plain and unauthenticated. A breakdown of the protection level for MAC management messages is provided in Table 7.

Table 7. Protection summary for IEEE 802.16-2009 MAC control messages.

Total Defined Management Messages	71
Reserved Messages	9
Total Non-Reserved	62
Authenticated Messages	30
Non-Authenticated	32

As the CMAC/HMAC protection is deemed effective, we regard messages protected as such to be free from exploitation as well as any modifications. For the MAC management messages that are not fully protected, we examined the characteristics and workings of each message in detail to ascertain possible exploitations. A summary of this assessment is provided in Table 8.

Table 8. Exploitation summary of IEEE 802.16-2009 MAC control messages.

Total Messages Protected	32
Limited Exploitation Scope	14
Messages With Possible Exploitation	18

The messages in Table 8 are then further categorized according to attack nature as well as functional group; they are listed in Table 9. A further distinction is made between vulnerabilities that have been previously identified in literature and those that have not.

The details of the preceding exploits are discussed in the next chapter, with emphasis on selected categories of attack. Most of the vulnerabilities identified involve injecting spoofed MAC control messages to the ABS or the AMS.

Table 9. Exploitation summary of IEEE 802.16-2009 MAC control messages according to types and functional groups.

Attack Nature/ Functional Group	Discussed in Literature	Current Discussion	Total
General Message Modification Attacks	3	5	8
Power Related Message Modification Attacks	1	0	1
MIMO Related Message Modification Attacks	0	1	1
Flooding Attacks	0	2	2
Water Torture Attacks	1	1	2
ARQ	1	2	3
AAS	0	1	1
Total Possible Exploitations	6	12	18

THIS PAGE INTENTIONALLY LEFT BLANK

IV. SPOOFING AND INJECTING CONTROL MESSAGES IN A TDMA REGIME

A. BACKGROUND

Most vulnerabilities involve an intruding station (IS) spoofing false MAC management messages at the ABS or an AMS. In contention based wireless standards such as IEEE 802.11 (Wifi), knowing the frequency and key parameters is sufficient for an attacker to start injecting messages. The TDMA and OFDMA nature of WiMAX means that in addition to knowing normal parameters, transmitting on the correct subcarriers and correct timing is also crucial. Most of the literature discusses vulnerabilities of MAC management messages, assuming they can be injected successfully without discussing details. Boom correctly identifies the single biggest challenge to mounting attacks on TDMA systems as timing [12].

In this chapter, we examine in detail the challenges and propose solutions to injecting MAC management messages, both at ABS and AMS. This material aims to give us some assurance that injection of messages at the physical level is feasible before MAC level attacks are discussed in the next chapter.

B. PREPARATION

1. Downlink Synchronization

Just like any other legitimate AMS joining a network, our IS needs to detect ABS transmission, acquire key system parameters, and perform downlink synchronization. This enables the IS to properly receive, demodulate, and interpret data transmitted by the ABS. For IEEE 802.16m, key steps include reading key parameters off the PA-Preamble and SA-Preamble and achieving downlink time synchronization. The IEEE 802.16m WiMAX frame is illustrated in Figure 35.

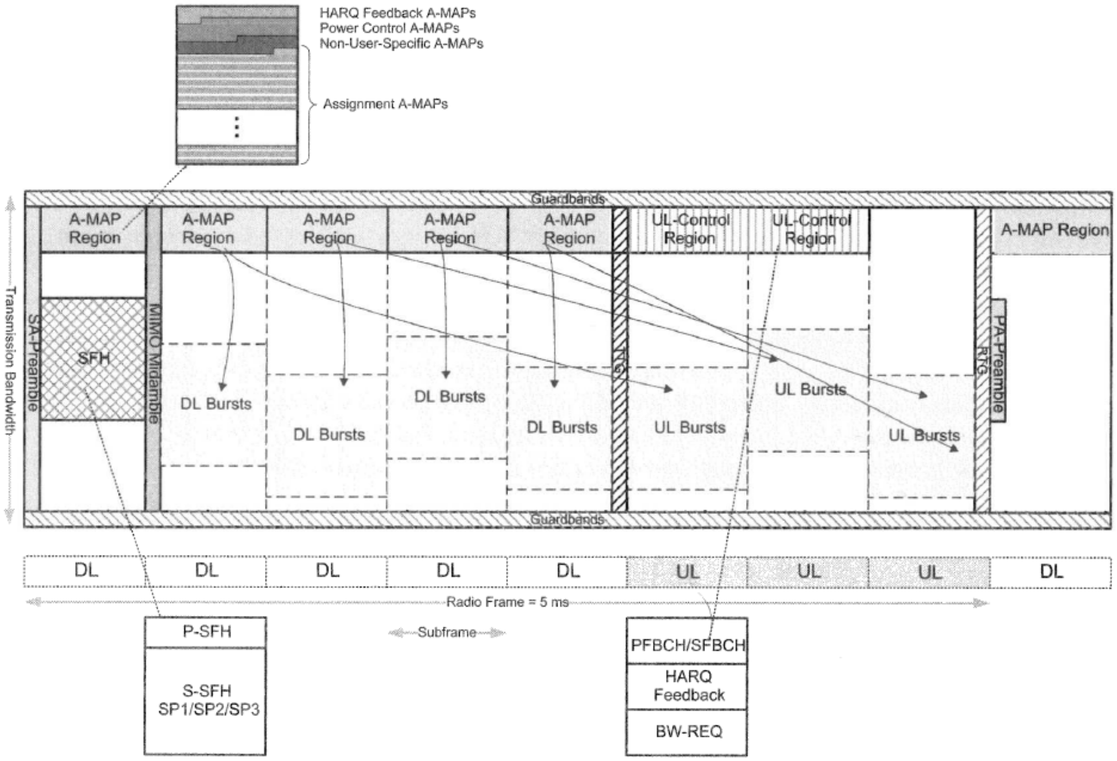


Figure 35. IEEE 802.16m frame with locations of PA-preamble and SA-preamble (From [14]).

As for legacy systems, key parameters need to be read from the preamble and time must be synchronized. The legacy WiMAX frame is illustrated in Figure 36.

2. Decode DL-MAP and UP-MAP and Eavesdrop on Control Traffic

In order to know where all bursts are located, the IS needs to decode the downlink medium access protocol (DL-MAP) as well as uplink medium access protocol (UL-MAP). For IEEE 802.16m, this information resides within the assignment A-MAP, as described in section II.C.7. Only the MAPs for broadcast traffic are available in plain, while MAPs for unicast traffic have been scrambled with a sequence derived from the AMS's STID and the MAPMask seed; both STID and the MAPMask seed were sent to each AMS through an encrypted channel during network entry (as described in section II.D). If an attacker is able to overcome the scramble, the unicast assignment A-MAP is available. Otherwise, only broadcast assignment A-MAP is available and only broadcast messages can be monitored and exploited.

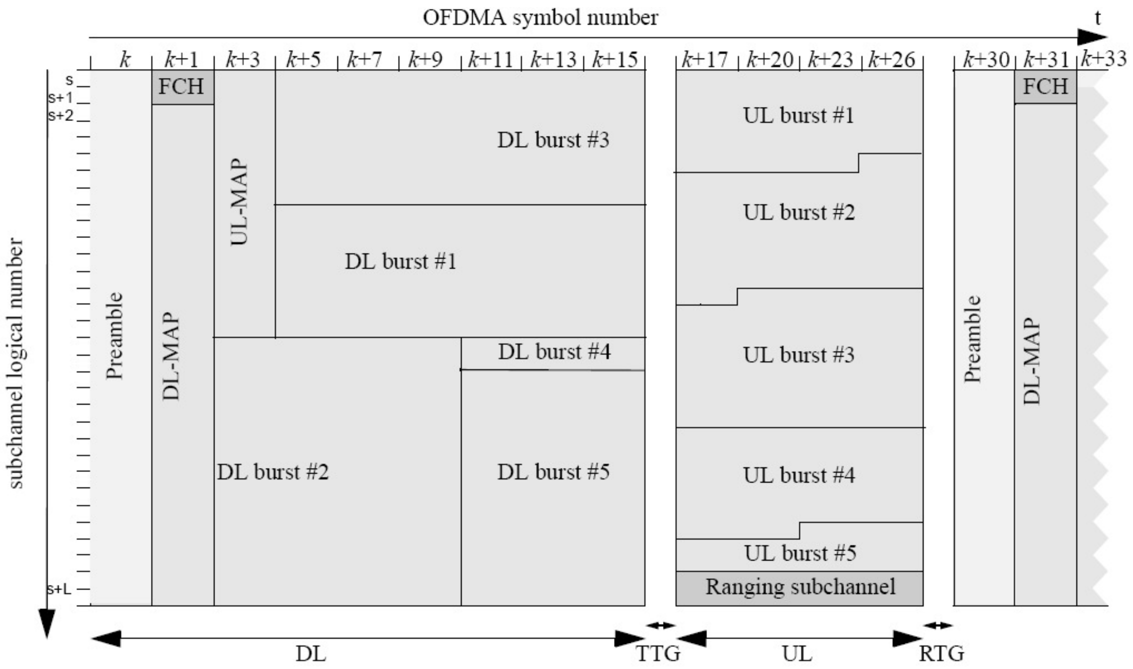


Figure 36. Legacy WiMAX frame (From [20]).

For legacy systems, the IS should: read key parameters from the frame control header (FCH), read DL-MAP to know timing and subcarriers used for bursts destined for each AMS, and read UL-MAP to know timing and subcarriers used for bursts transmitted by each AMS due for the ABS (the start point and area described in terms of symbol and subchannels). In this case, both unicast and broadcast MAPs are in plain. Within the DL-MAP and UL-MAP, the CID is the primary index to indicate ownership of each information element within the legacy WiMAX frame [20]. One such example is illustrated in Figure 37.

For both IEEE 802.16m and legacy systems, sub-channelization effects (as described in section II.C.3) also need to be taken into account, mapping logical resource units (LRUs) into physical resouce units (PRUs).

Once downlink synchronization and the decoding of MAPs are completed, the IS can listen and monitor some or all unencrypted traffic within the cell or sector.

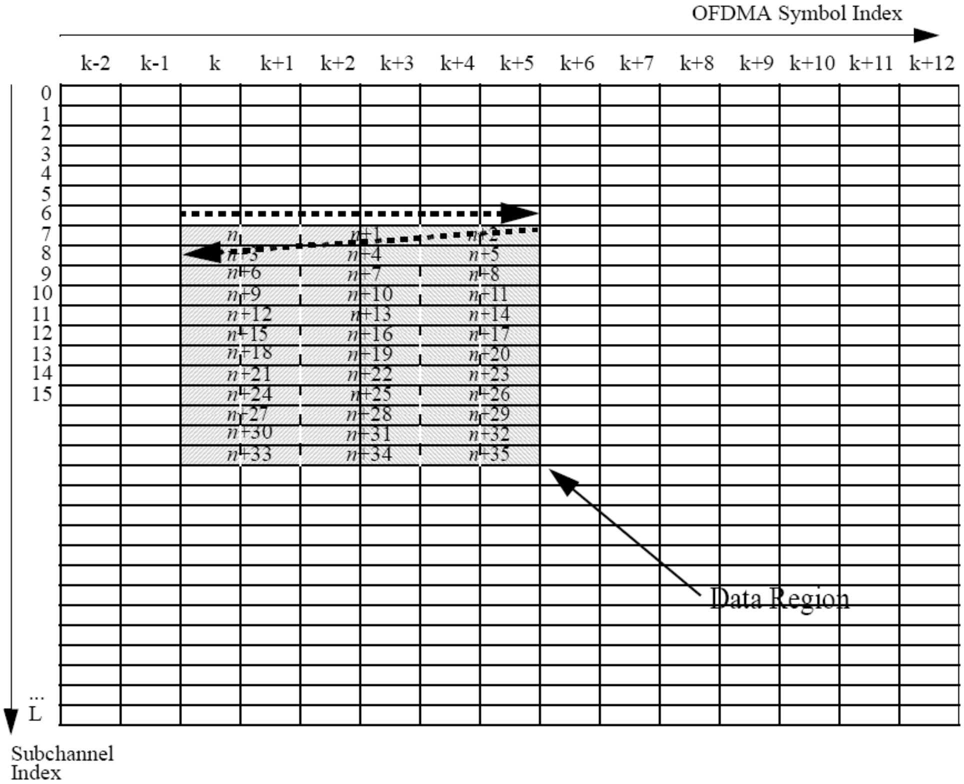


Figure 37. Example of data burst within legacy WiMAX frame (From [20]).

3. Listen for MS Joining Network and Intercept Connection ID (CID) if Subject of Interest is Unicast Message

In the case of legacy systems, the IS can listen for the CID issued by the BS to a joining MS through the relevant field within the RNG-RSP MAC management message sent from the BS to the MS as part of its joining process. The CID is important to identify the source and destination of messages, as well as to know which burst to target. For broadcast messages within both IEEE 802.16m-2011 and legacy systems, STID or CID is not required.

4. Acquire and Monitor ARQ Parameters and Numbers

Besides other parameters, the ARQ parameters in use are important; they allow the intruding system (IS) to properly formulate injected messages to ensure they are contextualized. The ARQ sequence number for each CID or broadcast message that we have an interest in needs to be tracked so that the sequence number in our injected message is acceptable.

C. PURPOSE OF RANGING AND CHALLENGES OF INJECTING MESSAGES WITHIN TDMA SYSTEMS

1. Ranging in TDMA Systems

Timing and burst allocation within the WiMAX frame is specifically assigned to each AMS within the UL-MAP and DL-MAP or assignment A-MAP. These timings are with reference to the ABS. This essentially means the timings meant for the commencement of transmission and reception are from the viewpoint of the ABS. For the downlink transmission, this means that propagation delays occur before reception at the AMS. The length of propagation delay is dependent on the distance of the AMS from the ABS. The AMS can achieve downlink synchronization through the pre-amble. Similarly, for the uplink, propagation delays occur between the time the AMS starts transmitting to the time the signal arrives at ABS. This arrival time needs to be referenced to the ABS's timing. To achieve this, the AMS needs to advance the start of transmission by a period equivalent to the propagation delay. Ranging is the process of ascertaining as well as fine-tuning timing adjustment. The schematic explaining the need for timing adjustment is illustrated in Figure 38. The section on the left depicts a scenario without timing adjustment, while the section on the right shows how timing adjustment enables the frame transmitted by the MS to arrive at the expected timing at the BS.

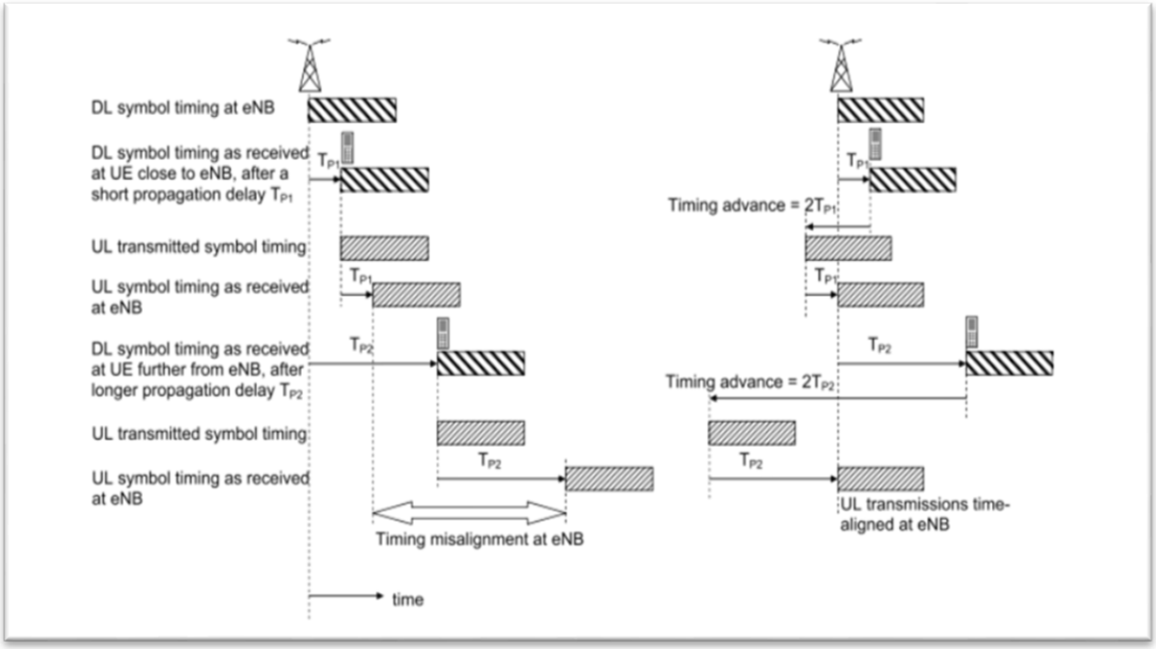

DL symbol timing at eNB
DL symbol timing as received at UE close to eNB, after a short propagation delay T_{P1}
T_{P1}
UL transmitted symbol timing
T_{P1}
UL symbol timing as received at eNB
DL symbol timing as received at UE further from eNB, after longer propagation delay T_{P2}
T_{P2}
UL transmitted symbol timing
T_{P2}
UL symbol timing as received at eNB
Timing misalignment at eNB
time
T_{P1}
Timing advance = $2T_{P1}$
T_{P1}
T_{P2}
Timing advance = $2T_{P2}$
T_{P2}
UL transmissions time-aligned at eNB

Figure 38. Ranging and timing adjust (From [21]).

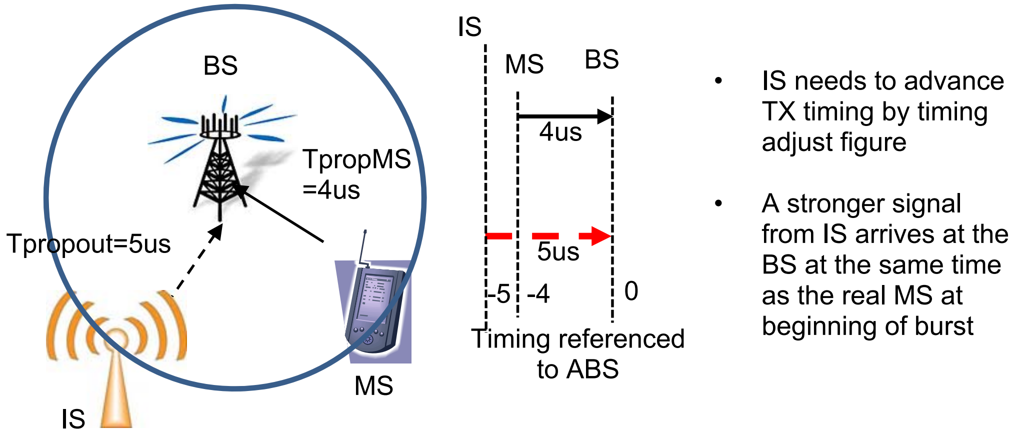
2. Challenges of Injecting Messages

The challenge of injecting messages within a TDMA system lies in establishing the correct timing adjustment to commence transmission at our IS to ensure that the signal arrives at the intended slot allocated for the ABS or AMS. As a perpetuator, although we may be able to perform ranging to obtain a timing adjust for uplink attacks, we will not have the benefit of ranging for downlink attacks involving another AMS. If the location of the AMS we are targeting is unknown, the challenge is even greater. Existing literature either assumes that this can be done or acknowledges the challenges without discussing solutions. To have some certainty that the proposed MAC message based attacks can work, a series of possible measures to overcome these timing requirements are proposed for different scenarios.

D. INSERTION OF MAC CONTROL MESSAGES

1. From Mobile Station to Base Station

This scenario is for the case when we attempt to spoof a MAC message from an AMS to ABS on the uplink. For the case of IEEE 802.16m-2011, unless the STID and MAPMask seed constraints discussed earlier can be overcome, the unicast UL-MAP cannot be read from the assignment A-MAP, and the message cannot be inserted. Although broadcast A-MAP can still be read, there is no broadcast traffic for uplink. A schematic of the scenario is provided in Figure 39. In this example, the MS need to advance transmission timing by 4us for the packet to reach the BS at the expected timing. As the IS is farther away from the BS, it needs to advance the transmission of its spoofed packet by 5us to ensure it can arrive at the expected time.



- IS needs to advance TX timing by timing adjust figure
- A stronger signal from IS arrives at the BS at the same time as the real MS at beginning of burst

Figure 39. Schematic and example of AMS to ABS scenario.

a. Locate Target Uplink Burst from UL-MAP

The IS first needs to ascertain the uplink burst location that is allocated to the AMS by the ABS for the current frame. In the case of legacy systems, this can be done by scanning the UL-MAP and looking for CIDs associated with the targeted AMS to determine the allocated transmission slots.

b. Establish Uplink Timing Adjustment through Initial Ranging

Once the target timing is ascertained, the IS needs to advance the transmission timing equivalent to the propagation delay between the IS and BS. In order to know how much to advance, the IS can perform an initial ranging (just as a normal AMS does to join the network) with the ABS. It does so by issuing an AAI-RNG-REQ (RNG-REQ for legacy systems) management message to the ABS on the ranging contention channel. The ABS performs measurements on the received signals and responds with timing and power adjust figures in AAI-RNG-ACK. The initial ranging process is shown in Figure 40. An equivalent process exists for legacy systems, with CID issued instead of STID/TSTID.

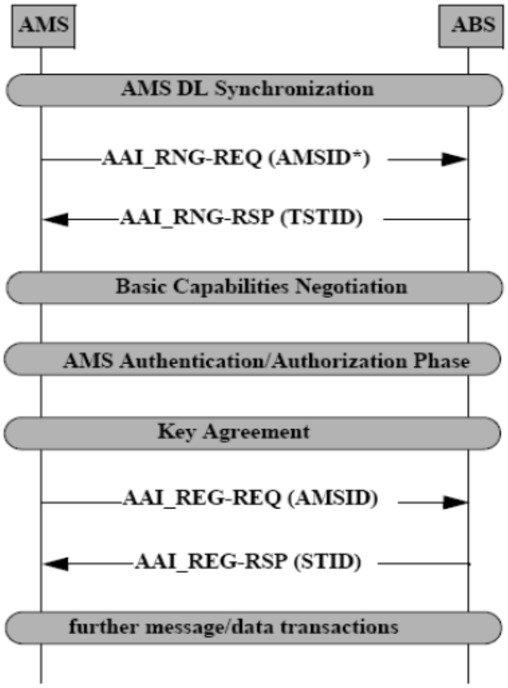


Figure 40. Network entry process with initial ranging (from [15] section 16.2.5.3.2).

c. Transmit Injected MAC MSG

The IS can then formulate the MAC management message, encapsulate it with a generic MAC header (GMH) and CRC at the tail (optional) to form a MAC management frame, and transmit it with a timing adjustment so that it will arrive at the same slot as the burst destined for the targeted AMS. The injected MAC frame has to commence at the very beginning of the traffic burst. This is preferred to injecting into the middle of a burst as to do that, the attack must know the contents of the burst before and after the injected symbols. To ensure that our signal can drown out that of the targeted AMS at the ABS, the IS has to transmit at a power higher than the resultant figure after incorporating the power adjustment figure from ABS. The transmit power level is discussed in a subsequent section.

d. Verify Effectiveness of Attack

The IS can then monitor traffic from the ABS and AMS to determine if the attack was successful.

e. ARQ Considerations

The implications of the ARQ mode as well as parameters in-force have to be considered when formulating the MAC message and encapsulating frame. Assuming the timing is correct and the frame is decoded at the ABS, in order for the MAC management message to be accepted, we have to meet ARQ conditions. This means that CRC checks have to pass and that the whole ARQ block containing our MAC management message has to be assessed by the ABS as intact. Otherwise, this frame could be discarded and a retransmit request sent out to the targeted MS. At some point after we stop our transmission and the signal from targeted AMS starts to be received by the ABS, CRC will fail and the ARQ will trigger, but this failed block must not contain our MAC management message. This essentially means that our injected message(s) and frame have to be sufficiently long (See Figure 41). The ARQ sequence number also needs to continue from the last sequence number used during the previous burst.

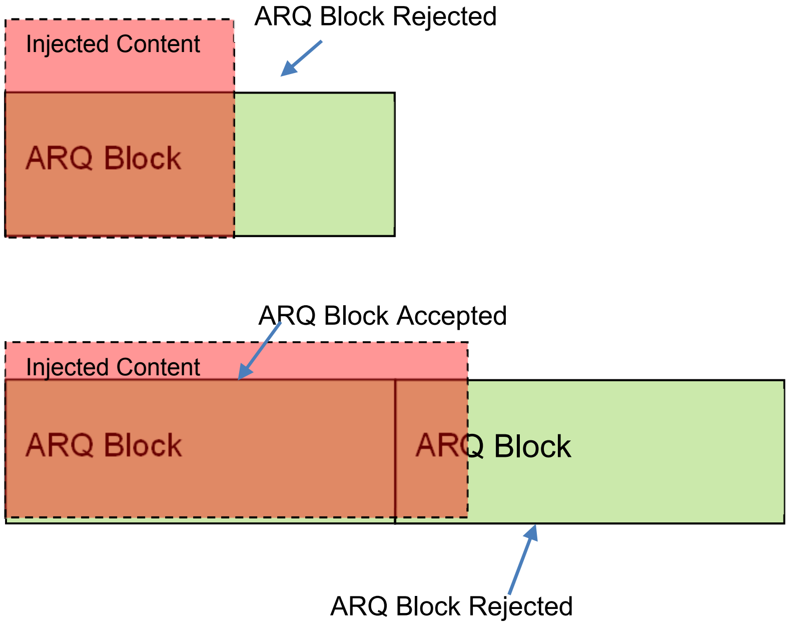


Figure 41. Ensuring injected content span across ARQ block.

f. Transmit Power

Due to the TDMA nature of WiMAX, our injected MAC message has to arrive at the victim's location at approximately the same time as the genuine signal. For our signal to override the genuine one, our signal strength needs to be higher. With power adjustment results obtained from the ranging process, the IS will know what transmission power to use to result in a nominal signal power at the ABS. This is computed by applying the power adjust figure (P_{Adjust}) to the power transmitted (P_{TX}) for the ranging ($P_{Initial\_Ranging}$). It is further proposed that an overpower gain ($G_{overpower}$) dependent on the modulation scheme be applied to transmission power. This overpowering gain is set according to the signal-to-noise ratio (SNR) requirement of the respective modulation scheme. The above computations are defined by

$$P_{TX}\,(dB) = P_{Initial\_Ranging} + P_{Adjust} + G_{overpower}. \qquad (1)$$

The net effect that we desire to achieve is to force the victim's automatic gain control to reduce gain and render genuine AMS's transmission to appear as noise in comparison to our signal while meeting requirements for SNR for the modulation scheme in use.

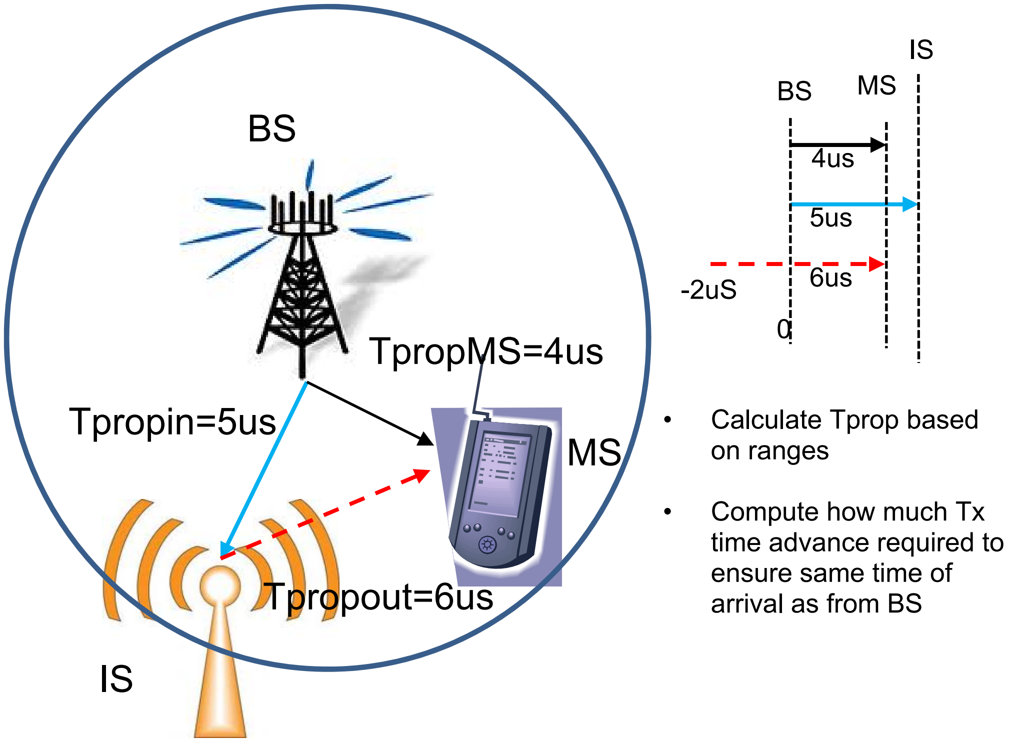
2. From Base Station to Mobile Station

This scenario is for the case where we attempt to spoof a MAC message from an ABS to AMS on the downlink. For the case of IEEE 802.16m-2011, unless the STID and MAPMask seed constraints as discussed earlier can be overcome, the unicast UL-MAP cannot be read from the assignment A-MAP and the message cannot be inserted. Broadcast A-MAP can still be read, and broadcast traffic can apply for downlink. The same basic principles and challenges from AMS to ABS scenario apply for the ABS to AMS scenario, but additional challenges emerge. In the previous scenario, signal injection was from IS to ABS, whereas in this scenario, our IS needs to inject signals to an AMS that is mobile, and its location may be unknown. To make matters worse, ranging cannot be carried out to ascertain distance and propagation delay, or power. The following discussion is set for two sub-scenarios: MS location known and MS location unknown.

a. Mobile Station Location Known

If the location of the mobile station that we plan to inject a message into is known, the timing adjustment required can be accurately estimated. A schematic of an ABS to AMS scenario with AMS position known is provided in Figure 42, which incorporates an example of how the location can be used to translate into propagation timings and how timing adjustments can be formulated.

i. Locate Targeted Downlink Burst from DL-MAP. The IS first needs to ascertain the downlink burst location allocated by the ABS to transmit to AMS for the current frame. This can be done by scanning the assignment A-MAP or DL-MAP for slots allocated for the ABS to transmit to targeted AMS.



- Calculate Tprop based on ranges
- Compute how much Tx time advance required to ensure same time of arrival as from BS

Figure 42. Schematic and example of ABS to AMS scenario.

ii. Compute Downlink Timing Adjust. Once the targeted timing with reference to ABS is ascertained, the IS needs to advance or delay transmission timing. The IS can compute a timing adjustment by computing the distance between ABS and AMS and between IS and AMS. The difference in distance, converted to the corresponding timing, is the timing adjustment.

iii. Transmit Injected MAC MSG. The IS can then formulate the MAC management message, encapsulate it with a GMH and CRC at the tail (optional) to form a MAC management frame, and transmit it with timing adjustment so that it arrives at the slot destined for the targeted AMS. The injected MAC frame has to commence at the very beginning of the traffic burst. This is to minimize the amount of context that we need to deal with if we inject mid-frame.

iv. Verify Effectiveness of Attack. The IS can then monitor traffic from the ABS and AMS to determine if the attack was successful.

v. ARQ Considerations. The implications of the ARQ mode and parameters in force have to be considered when formulating the MAC message and encapsulating frame. Assuming the timing is correct and the frame is decoded at the AMS, for the MAC management message to be accepted, we have to meet ARQ conditions. This means that CRC checks have to pass and that the whole ARQ block containing our MAC management message has to be assessed by the AMS as intact. Otherwise, this frame could be discarded and a retransmit request sent out to the ABS. At some point after we stop our transmission and the signal from ABS starts to be received by the AMS, CRC will fail and ARQ will trigger, but this failed block must not contain our MAC management message. This essentially means that our injected message(s) and frame have to be sufficiently long. The ARQ sequence number also needs to continue from the last sequence number used during the previous burst.

vi. Uncertainty Analysis. As no ranging was performed, the timing adjustment is worked out using the GPS coordinates of the ABS, IS, and AMS. These position estimates have their own tolerances. Hence, an analysis is carried out to confirm timing margins and the feasibility of success. For a commonly adopted configuration, the OFDMA symbol duration is 91.4 us, preceded with a guard interval (t_{GI}) of 11.4 us, padded with a cyclic prefix. Timing uncertainties in this situation are tabulated in Table 10.

Table 10. Timing uncertainty computation

Factor	**Uncertainty**	$\mathbf{t_{error}}$
BS GPS Position Uncertainty	5m	16.7ns
MS GPS Position Uncertainty	5m	16.7ns
IS GPS Position Uncertainty	5m	16.7ns
Max Position Uncertainty		**50.1ns**
Channel Spread (Max)		**4us**
Total Uncertainty	-	**4.05us**
Guard Interval		**11.4us**
Margin	-	**7.35us**

As seen from the computation, after taking into account the positional uncertainty (from the GPS position uncertainty [22]) of the ABS, AMS, and IS, as well as the channel spread, we have a margin of 7.35 us (see Figure 43). Hence, a foreseeable timing error of a frame injection at the beginning of a burst is not major factor as this error is less than the difference between the maximum delay spread and the guard interval.

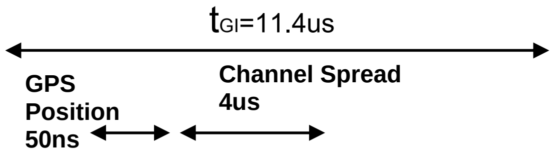


Figure 43. Illustration of timing uncertainty vs guard interval.

vii. Transmission Power. Due to the TDMA nature of WiMAX, our injected MAC message has to arrive at the victim's location at approximately the same time as the genuine signal. For our signal to override the genuine one, its signal strength needs to be higher. The approach taken to estimate the transmission power for this scenario is different. The IS will measure incident power from the ABS ($P_{ABS(incident)}$). With the distance from the ABS to IS known, the path loss (L_{ABS-IS}) can be estimated, and hence, transmission power for the ABS can be estimated. Likewise, with the distance from the ABS to the

AMS known, path loss ($L_{ABS\text{-}AMS}$) can be estimated. Hence, the estimated transmission power by the ABS incident upon the targeted AMS can be obtained. Next, the path loss between the IS and AMS ($L_{IS\text{-}AMS}$) needs to be factored in. It is also proposed that an overpower gain ($G_{overpower}$) which is dependent on the modulation scheme be applied to the transmission power. This overpower gain is set according to the SNR requirement of the respective modulation scheme. Hence, the proposed transmission power is computed according to

$$P_{TX}\ (dB) = P_{ABS(incident)} + L_{ABS\text{-}IS} - L_{ABS\text{-}AMS} + L_{IS\text{-}AMS} + G_{overpower}. \qquad (2)$$

The desired net effect of the proposed transmission power is to force the victim’s automatic gain control to reduce gain and render the genuine source’s transmission to appear as noise in comparison to our signal while meeting the SNR requirements for the modulation scheme in use.

b. Mobile Station Location Unknown

If the location of the mobile station that we plan to inject a message into is unknown, we can attempt transmission of the injected message over multiple attempts over a selected range which is bounded by the cell dimension. A schematic showing an ABS-to-AMS scenario with MS position unknown and cell size of 5 km is provided in Figure 44. As shown in the figure, there are two extreme scenarios in terms of the distance from the AMS to IS. The AMS and IS could be at the edge of the cell (far case) or right next to each other (near case).

i. Locate Target Downlink Burst from DL-MAP. The IS first needs to ascertain the downlink burst location allocated by the ABS to transmit to the AMS for the current frame. This can be done by scanning the assignment A-MAP or DL-MAP for slots allocated for the ABS to transmit to the targeted AMS.

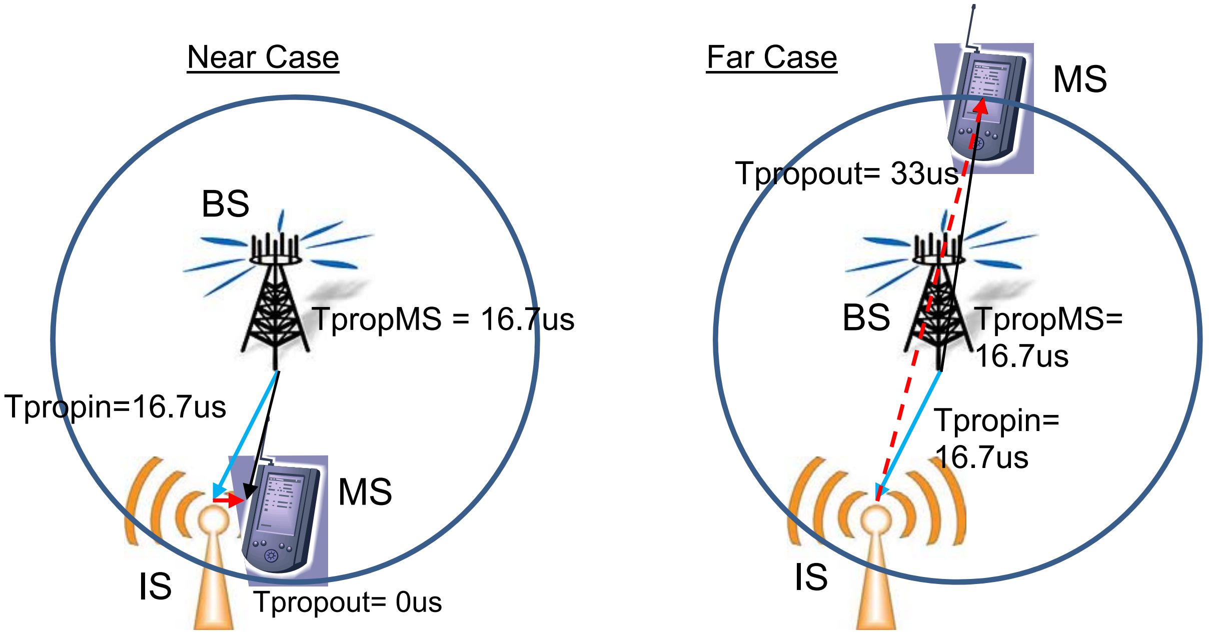


Figure 44. Example illustrating a scenario of injection to MS with unknown position.

ii. Compute Downlink Timing Adjust. Once the target timing is ascertained, the IS needs to compute the possible ranges for the timing adjust to attempt. Let $t_{prop(max)}$ be the propagation delay for the worst case whereby the IS and AMS are at the extreme ends of the cell (far case in Figure 44). For the far case, the timing needs to be advanced by half of $t_{prop(max)}$. This ensures that the injected signal has sufficient time to propagate across the cell and arrive at the AMS at approximately the same time as the signal from ABS. For the near case, the timing needs to be delayed by half of $t_{prop(max).}$ This is because the signal transmitted to the AMS takes that length of time to propagate to the edge of the cell. For different positioning of the AMS and IS, the timing adjustment will vary between the two extreme cases (far and near cases) For different positioning of the AMS and IS, the timing adjustments will vary between the two extreme cases. The above concepts are illustrated in Figure 45.

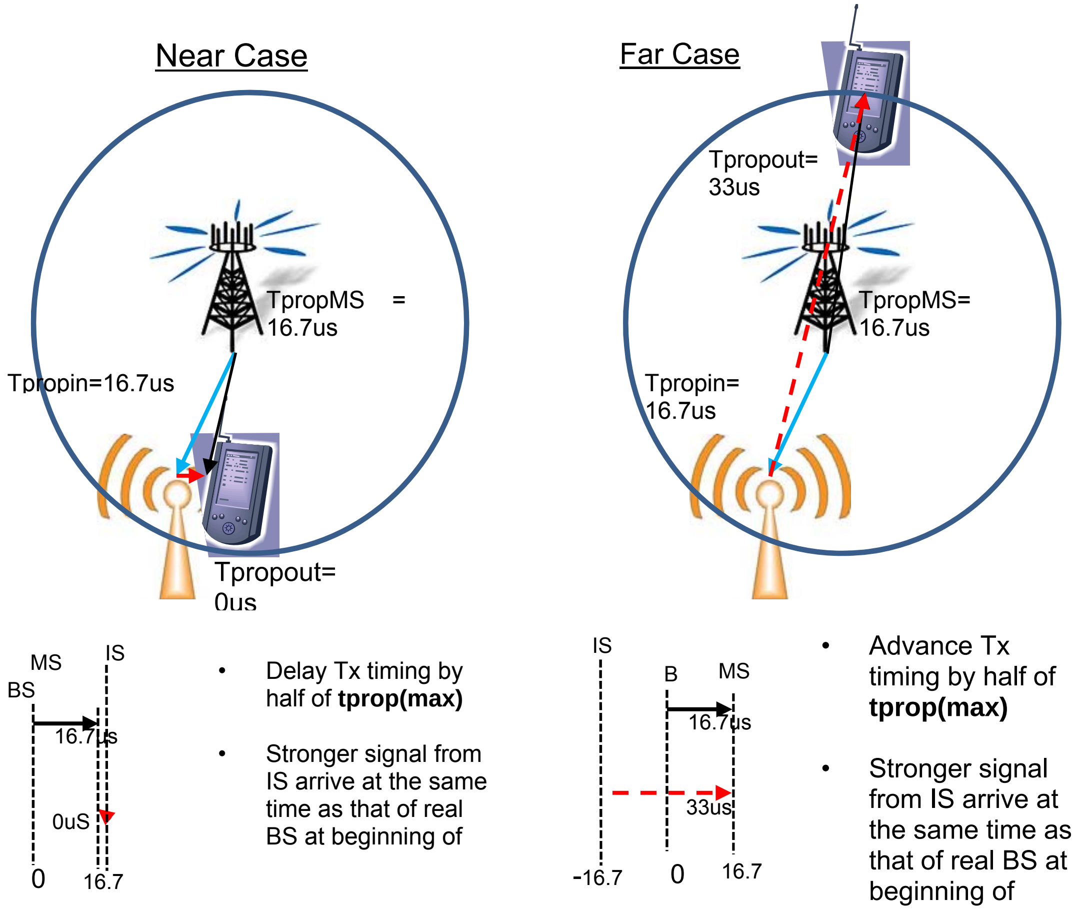

Near Case
TpropMS =
16.7us
Tpropin=16.7us
Tpropout=
0us
Far Case
Tpropout=
33us
TpropMS=
16.7us
Tpropin=
16.7us
MS
BS
IS
16.7μs
0uS
0
16.7
Delay Tx timing by half of **tprop(max)**
Stronger signal from IS arrive at the same time as that of real BS at beginning of
IS
B
MS
16.7us
33us
-16.7
0
16.7
Advance Tx timing by half of **tprop(max)**
Stronger signal from IS arrive at the same time as that of real BS at beginning of

Figure 45. Illustration of implication of unknown AMS location on transmit timing.

Once the range of possible timings has been computed, the next step is to divide the range into intervals with each interval being $t_{GI}/2$ where t_{GI} is the duration of the guard interval. How the possible timing range and intervals can be selected around the expected timing of the burst commencement is illustrated in Figure 46. This expected timing should be referenced to the BS (timing at IS minus propagation delay from ABS to IS). The central idea is to attempt injection at different times within the range, selecting one interval per frame until the timing falls within the actual guard interval and the MAC message is accepted. An interval of $t_{GI}/2$ ensures that the IS will not inadvertently skip over the actual guard band. The IS can measure the incident power of pilot carriers from the targeted AMS. From the measured power, it can estimate the distance of AMS from IS by assuming path loss using the free-space model. With this estimated distance, the IS can select a better timing interval to begin the message injection. This should improve the probability of early success.

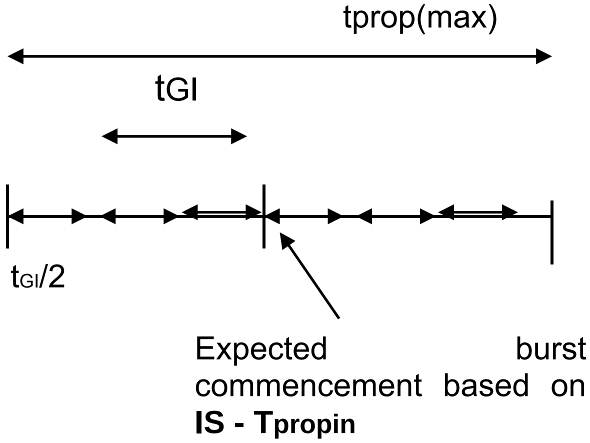


Figure 46. Example of MAC message injection plan.

iii. Transmit Injected MAC MSG. The IS can then formulate the MAC management message, encapsulate it with a GMH and CRC at the tail (optional) to form a MAC management frame, and transmit it with a timing adjustment so that it arrives at the same slot destined for the targeted AMS. The injected MAC frame has to commence at the very beginning of the traffic burst. This is to minimize the amount of context we will need to deal with if we inject mid-frame.

iv. Verify Effectiveness of Attack. After the attempted injection of a MAC message at one of the intervals within the range, the IS can monitor traffic from the ABS and AMS during the next frame to determine if the attack was successful.

v. ARQ Considerations. As in the above scenarios, the implications of the ARQ mode and the parameters in-force have to be considered when formulating the MAC message and encapsulating frame. Assuming the timing is correct and the frame is decoded at the victim, for the MAC management message to be accepted, we have to meet ARQ conditions. This means that CRC checks have to pass and that the whole ARQ block containing our MAC management message has to be assessed by the victim as intact. Otherwise, this frame could be discarded and a retransmit request sent out to the source. At some point after we stop our transmission and the signal from the source starts to be received by the victim, the CRC will fail and the ARQ will trigger, but this failed block must not contain our MAC management message. This essentially means that our injected message(s) and frame have to be sufficiently long. The ARQ sequence number also needs to continue from the last sequence number used during the previous burst.

vi. Transmission Power. Due to the TDMA nature of WiMAX, our injected MAC message has to arrive at the victim's location at approximately the same time as the genuine signal. For our signal to override the genuine one, our signal strength needs to be higher. The approach taken to estimate the transmission power for this scenario is different, as the distances between AMS and IS and between ABS and AMS are unknown. In this case, the path loss between the IS and targeted AMS ($L_{IS\text{-}AMS}$) is estimated since the distance is unknown. The distance between the ABS and IS as well as the incident ABS power ($P_{ABS(incident)}$) measured at the IS are used to estimate the transmission power of the ABS. Since the distance between the ABS and AMS is unknown, the worst case is assumed where the AMS is co-located with ABS. Therefore, full ABS transmission power is incident upon the AMS (where the $L_{ABS\text{-}AMS}$ term in Equation (2) is zero in this scenario). Thus, the ABS transmission power, together with the path loss associated with the timing currently being attempted, is used to compute the IS transmission power (P_{TX}). It is also proposed that an overpower gain ($G_{overpower}$), which is dependent on the modulation scheme in-use, be applied to the transmission power. This overpower gain is set according to the SNR requirement of the respective modulation scheme. The proposed transmission power is calculated according to the following:

$$P_{TX}\ (dB) = P_{ABS(incident)} + L_{ABS\text{-}IS} + L_{IS\text{-}AMS} + G_{overpower}. \qquad (3)$$

The desired net effect of the proposed transmission power is to force the victim's automatic gain control to reduce gain and render the genuine source's transmission to appear as noise in comparison to our signal while meeting the SNR requirement of the modulation scheme in use.

V. ATTACKS BASED ON MANIPULATION OF UPLINK TRANSMISSION POWER WITH IEEE 802.16M-2011

A. BACKGROUND

Having proposed the means to inject MAC management messages, we proceed to discuss a class of attack which involves the injection of messages to manipulate the uplink power control of AMSs within a WiMAX cell. Proper power management is vital to the correct operation of a WiMAX cell. Low transmission power results in high bit error rates or no reception. Excessively high transmission power also results in interference to nearby cells using the same set of frequencies. Both effects are disruptive to the targeted network's operations. Depending on the selected attack vectors, the effects could be surgical and covert, targeting a single AMS, or blanket, disrupting all nodes within a cell. IEEE 802.16m-2011 power related attacks are addressed in this chapter. Those for legacy systems are addressed in a later chapter.

B. UPLINK POWER CONTROL

Overall network uplink power control can be summarized from [15] section 16.3.8.4 in Figure 47.

In Figure 47, there are three stages in uplink power control, initial network entry, normal network operations, and handover. In the following subsections, an overview of their functionalities is given which provide the background to understanding the attack methodologies presented in the later chapters of this thesis.

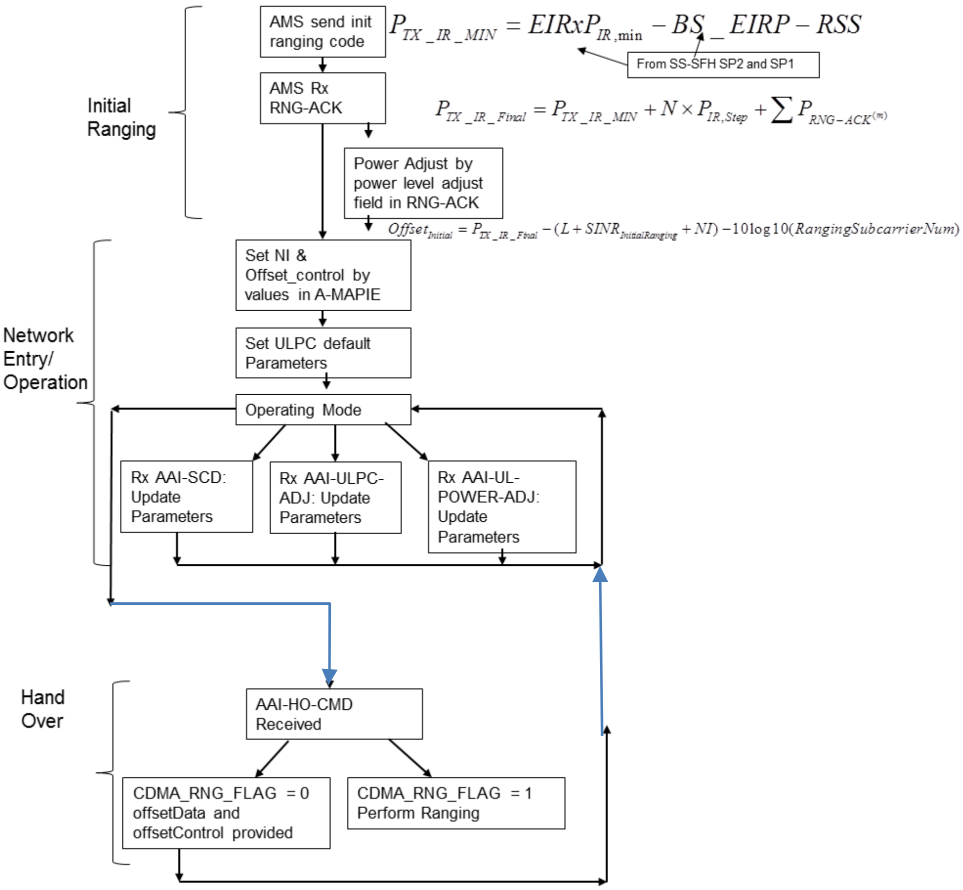

Initial Ranging
AMS send init ranging code
$P_{TX\_IR\_MIN} = EIRxP_{IR,\min} - BS\_EIRP - RSS$
From SS-SFH SP2 and SP1
AMS Rx RNG-ACK
$P_{TX\_IR\_Final} = P_{TX\_IR\_MIN} + N \times P_{IR,Step} + \sum P_{RNG-ACK^{(m)}}$
Power Adjust by power level adjust field in RNG-ACK
$Offset_{Initial} = P_{TX\_IR\_Final} - (L + SINR_{InitialRanging} + NI) - 10\log 10(RangingSubcarrierNum)$
Network Entry/ Operation
Set NI & Offset_control by values in A-MAPIE
Set ULPC default Parameters
Operating Mode
Rx AAI-SCD: Update Parameters
Rx AAI-ULPC-ADJ: Update Parameters
Rx AAI-UL-POWER-ADJ: Update Parameters
Hand Over
AAI-HO-CMD Received
CDMA_RNG_FLAG = 0 offsetData and offsetControl provided
CDMA_RNG_FLAG = 1 Perform Ranging

Figure 47. Summary of uplink power control.

1. Power Control during Initial Ranging

As discussed previously, an AMS attempting to join a network first performs downlink synchronization, which includes reading system parameters from the preamble, superframe headers, assignment A-MAPs, or UL-MAP and DL-MAP. The AMS then attempts to perform uplink synchronization, which includes initial ranging. The received signal strength (RSS) from ABS is first measured, and this figure is added to EIRxP$_{IR,min}$ and BS_EIRP, which are parameters present in SS-SFH SP2 and SP1, to obtain the initial transmission power that the AMS will use to transmit the initial ranging preamble to the ABS. This initial transmission power is calculated from

$$P_{TX\_IR\_MIN} = EIRxPI_{IR,\min} - BS\_EIRP - RSS \,. \qquad (4)$$

Should the ranging operation be successful, the ABS provides power adjustment figures to the AMS through the power level adjustment (or $P_{RNG\text{-}ACK}$) parameter within the AAI-RNG-ACK MAC management message. After *N* times of ramping up and *m* times of receiving AAI-RNG-ACK, the final initial ranging transmission power ($P_{TX\_IR\_Final}$) is

$$P_{TX\_IR\_Final} = P_{TX\_IR\_\_MIN} + N \times P_{IR,Step} + \Sigma P_{RNG-ACK^{(m)}} \qquad (5)$$

where $P_{IR,Step}$ is defined in IEEE 802.11m-2001 standard as 2 dB.

Hence, $\text{Offset}_{\text{Initial}}$ is defined as

$$\begin{aligned} Offset_{Initial} &= P_{TX\_IR\_Final} - (L + SINR_{InitialRanging} + NI) \\ &-10\log 10(RangingSubcarrierNum) \end{aligned} \qquad (6)$$

where *L* is the estimated average DL propagation loss calculated by AMS; *NI* is the estimated average noise and interference power per subcarrier at ABS as indicated by AAI-ULPC-NI message; and $SINR_{InitialRanging}$ is defined as

$$SINR_{InitialRanging} = offsetControl + \mathrm{targ}etInitialRangingSinr \qquad (7)$$

where $offsetControl$ is obtained from A-MAP Information Element (IE) and $\mathrm{targ}etInitialRangingSinr$ is defined in Table 946 in IEEE 802.16m-2011 standard.

2. Power Control during Network Entry and Normal Operations

After completion of initial ranging, NI and offsetControl are set as instructed by ABS through A-MAP. Other UL power control parameters are set to defaults as defined in Table 947 in IEEE 802.16m-2011 standard.

During normal operations, UL transmission power level is controlled by

$$P_T = P_L + SINR_{Tgt} + P_{NI} + P_{offset} \qquad (8)$$

where P_L, $SINR_{Tgt}$, P_{NI} and P_{offset} are defined and illustrated in Figure 48.

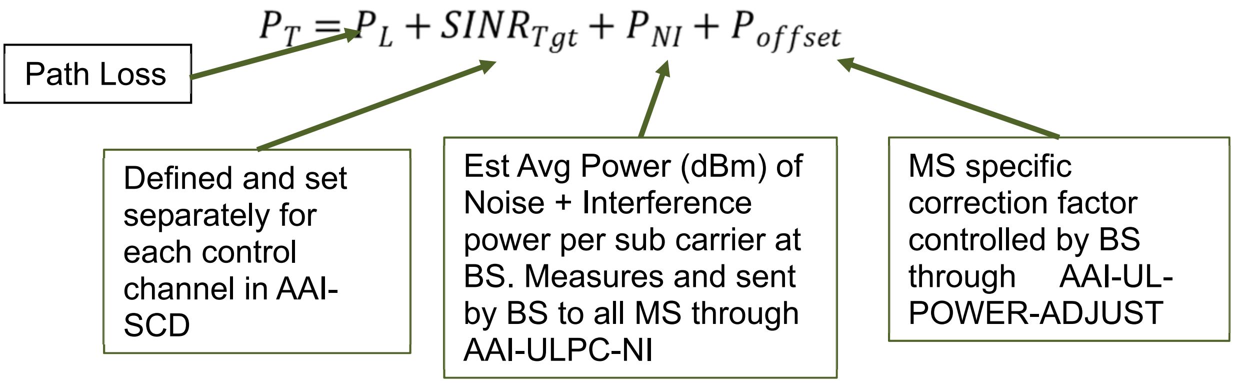

$P_T = P_L + SINR_{Tgt} + P_{NI} + P_{offset}$
Path Loss
Defined and set separately for each control channel in AAI-SCD
Est Avg Power (dBm) of Noise + Interference power per sub carrier at BS. Measures and sent by BS to all MS through AAI-ULPC-NI
MS specific correction factor controlled by BS through AAI-UL-POWER-ADJUST

Figure 48. Equation for MS uplink transmission power.

While this general equation holds true, different sets of P_{offset} and $SINR_{Tgt}$ values exist for different channels (e.g. control, data, and ranging channels).

There are two types of P_{offset} that are controlled by the ABS through the AAI-UL-POWER-ADJUST message: $Offset_{Control}$ and $Offset_{Data}$. The $Offset_{Control}$ parameter governs the control channels and is defined as

$Offset_{Control}$ = $Offset_{Initial}$ (discussed in previous section) + offsetControl (parameter in AAI-UL-POWER-ADJUST message) (9)

while the $Offset_{Data}$ parameter is used for data channels and is defined as $Offset_{Data} = Offset_{Initial}$.

There are two types of $SINR_{tgt}$; one governs the control channels and is supplied by the ABS through the AAI-SCD message, and the other one governs the data channels values and is defined in by

$$SINR_{tgt} = 10\log[\max(SINR_{\min}, \gamma SIR_{DL} - \alpha)] - \beta 10\log(n_{stream}) \qquad (10)$$

where $SINR_{tgt}$, $SINR_{min}$, γ, $SIR_{DL,}$ and α are defined and illustrated in Figure 49. The β value is a masking parameter set to zero or one for excluding or including the effects of n_{stream} where n_{stream} is the number of streams in the logical resource unit that is signaled by the uplink A-MAP.

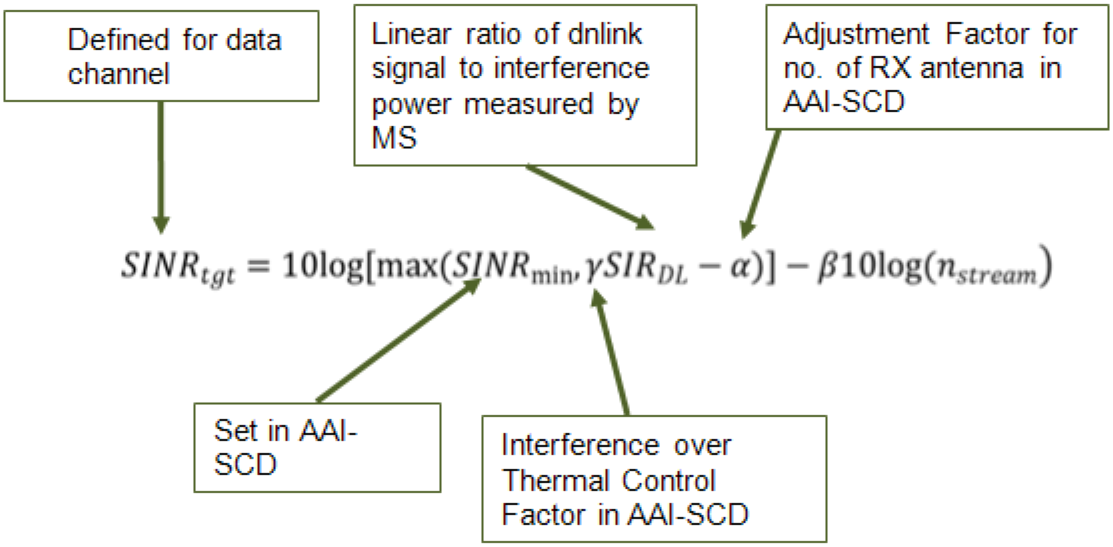

Defined for data channel
Linear ratio of dnlink signal to interference power measured by MS
Adjustment Factor for no. of RX antenna in AAI-SCD
$SINR_{tgt} = 10\log[\max(SINR_{\min}, \gamma SIR_{DL} - \alpha)] - \beta 10\log(n_{stream})$
Set in AAI-SCD
Interference over Thermal Control Factor in AAI-SCD

Figure 49. Equation for *SINR*$_{tgt}$ in uplink transmission power.

3. Power Control during Handover

During handover of an AMS from cell to cell, an AAI-HO-CMD message is received by the AMS. Within the message, the CDMA_RNG_FLAG indicates if it is necessary to conduct ranging. If CDMA_RNG_FLAG = 0, offsetData and offsetControl are provided within the message.

C. MANIPULATION OF POWER CONTROL

In the following subsections, possible approaches to manipulate the uplink transmit power of AMSs are discussed.

1. Manipulate P_{NI} for Entire Cell Through AAI-ULPC-NI

To reiterate, the transmission power at the AMS is governed by Equation (8).

One possible attack of uplink power management is to inject an AAI-ULPC-NI message with a small or large *NI* value. If a low value is injected, the SNR at ABS drops. Should the drop be large enough to cause the SNR to fall below the requirement for the modulation scheme in use, the bit error rate increases or reception may be eliminated altogether. If a large *NI* value is injected, the large signal strength may increase interference with cells in the vicinity using the same frequencies.

Although a single strong emission may not be a major problem for other cells, bear in mind that this message is broadcast and all AMSs within the cell may be affected under the right conditions, thus, greatly multiplying the effect. The parameter *NI* is defined as

$$NI = PTN + IoT + 10\log10(\Delta f) \qquad (11)$$

where *PTN* is the thermal noise power density at zero Celsius, which has a value of -174.2 dBm, and *Δf* is the subcarrier spacing (Hz), and *IoT* corresponds to *gammaIotFp0*, which is defined in Table 11.

To change the power, the *gammaIotFp0* field within AAI-ULPC-NI can be modified; it can be varied from 0 to 63.5 dB in 0.5 dB steps, which represent a dynamic range of 2.23x10^6. Details on this field are provided in Table 11. Both control and data channels are affected by this manipulation.

Table 11. *gammaIotFp* parameter within AAI-ULPC-NI.

Field	Size	Value/Description
gammaIotFp0	7	IoT value of Frequency Partition #0, quantized in 0.5 dB steps as IoT level from 0 dB to 63.5 dB.

AAI-ULPC-NI is a broadcast message, and all AMSs within the cell served by the ABS may be affected. Although all AMSs can potentially be affected, the timing adjustment from the IS to individual AMS also needs to be correct for the AMS to take in the broadcast correctly. The challenges brought about by differences in timing precipitated by the distance between the IS and ABS are illustrated in Figure 50. A broadcast signal (by IS) reaches AMSs over different locations at different times from a broadcast signal sent from the real ABS.

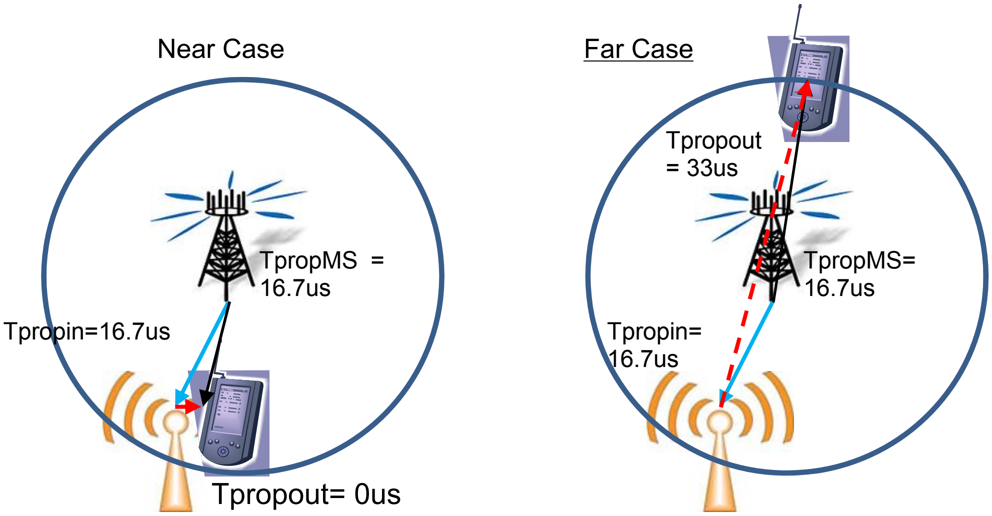


Figure 50. Timing differences for different AMS during broadcast message manipulation.

This might mean that if multiple AMSs within the cell need to be targeted, the spoofed message may need to be sent out repeatedly over several frames within a range of timing adjustments. Alternatively, the closer the IS is to the ABS, the smaller the maximum timing difference is. It is estimated that if the distance between the ABS and IS is within the distance equivalent to a propagation delay of one Cyclic Prefix (CP) (i.e.,11.42 us, which is equivalent to 3426 m), no timing adjustment is needed in order to affect all AMSs within the whole cell.

2. Manipulate P_{offset} For Single AMS through AAI-UL-POWER-ADJUST

To reiterate, the transmission power of an AMS is governed by Equation (8). Another possible attack of uplink power management is to inject an AAI-UL-POWER-ADJUST message with a low or high offsetData or offsetControl value. If a low value is injected, the SNR at ABS drops. Should the drop be large enough to cause the SNR to fall below that required for the modulation scheme, the bit error rate will increase or reception may be eliminated altogether. If a high offset value is injected, the high signal strength may increase interference for cells in the vicinity using the same frequencies. However, since this is a unicast message, only one AMS is affected by the message inject, and a single strong emission may not be a major problem for other cells. To cause a larger impact on other cells, multiple AMSs may need to be manipulated to multiply the effect.

The *offsetData* and *offsetControl* fields in the AAI-UL-POWER-ADJUST message can be varied from -15.5 to 16 dB in 0.5 dB steps, which represents a dynamic range of 2.23x10^6. Details on this field are provided in Table 12.

Table 12. Offset parameter within AAI-UL-POWER-ADJUST.

Field	**Size**	**Value/Description**
offsetData	6	offsetData is the transmission power adjustment value transmitted by the ABS. It represents the value among -15.5 to 16 dB with 0.5 dB step
offsetControl	6	offsetControl is the transmission power adjustment value transmitted by the ABS. It represents the value among –15.5 to 16 dB with 0.5 dB step

As discussed earlier, AAI-UL-POWER-ADJUST is a unicast message and only a single AMS will be affected per successful message injection. Offset values for control and data channels can be individually set, meaning that the data channel can be selectively targeted while leaving the control channels alone. This approach can disrupt network operations while making detection more difficult, as the affected AMS will appear to be functioning normally, because it is still responding to on the control channels.

For IEEE 802.16m, challenges still exist. Since AAI-UL-POWER-ADJUST is a unicast message, its A-MAP is scrambled as described in Sections II.C.7 and II.B.1. It is not readily accessible unless an algorithm is developed to overcome the scramble. Hence, injecting an AAI-UL-POWER-ADJUST poses a significant challenge as of now.

3. Manipulate *$SINR_{tgt}$*

To reiterate, transmission power at the AMS is governed by Equation (8). Another possible attack of uplink power management is to manipulate *SNR_{tgt}* by injecting an AAI-SCD message. The *$SINR_{tgt}$* parameter is defined in Equation (10). Details for three of the parameters in this equation are provided in Table 13.

Table 13. Details of key parameters of AAI-SCD.

Field	Size	Value/Description
gammaIotFp0	4	gammaIotFp (IoT) is the fairness and IoT control factor, broadcast by the ABS. It has 4 bits to represent the value among {0, 0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 1.0, 1.1, 1.2, 1.3, 1.4, 1.5}. It is different for each frequency partition (FP0, FP1, FP2, FP3).
Alpha	3	alpha (α) is the factor according to the number of receive antennas at the ABS. It has 3 bits to express {1, 1/2, 1/4, 1/8, 1/16, 0, reserved, reserved}
dataSinrMin	4	dataSinrMin is the SINR requirement for the minimum data rate expected by ABS. SINRmin_Data has 4 bits to represent the value in dB among{-INF, –3, –2.5,–2, –1.5, –1, –0.5, 0, 0.5, 1, 1.5, 2, 2.5, 3, 3.5, 4}

a. Manipulating dataSinrMin through AAI-SCD

With reference to Equation (10), it is possible to manipulate *$SINR_{tgt}$* by spoofing AAI-SCD with an amended *dataSinrMin*. However, due to the maximum function built into the equation, there is no effect if the other term is higher than the new dataSinrMin.

b. Manipulating gammaIotFpx through AAI-SCD

With reference to Equation (10), it is possible to manipulate *$SINR_{tgt}$* by spoofing AAI-SCD with an amended *gammaIotFpx*. However, due to the maximum function built into the equation, there is no effect if the other term is higher than the new value.

c. Manipulating alpha through AAI-SCD

With reference to Equation (10), $SINR_{tgt}$ can be manipulated by amending *alpha* within AAI-SCD. However, due to the maximum function built into the equation, there is no effect if the other term is higher than the new value.

4. Holistic Analysis of Power-Manipulation Options

A summary of power-related attacks is provided in Table 14. The analysis below compares the three key attack approaches:

a. Effect of Impact

The three approaches can achieve varying degrees of dynamic range, from 63.5 dB for *NI* within AAI-ULPC-NI to a factor of 1.5 for *gammaIotFp* in AAI-SCD. A higher dynamic range is desirable as this results in a more pronounced impact. Comparisons are shown in the Power Control Range column in Table 14. From the perspective of maximum impact, the approach involving the manipulation of P_{NI} is the most desirable.

b. Ease of Attack

Similarly, the three approaches have varying degrees of ease of execution, ranging from a simple and short MAC management message injection (for a message body of less than 50 bits) for manipulating P_{NI} within the AAI-ULPC-NI message to a moderately long (more than 200 bits) MAC management message modification when P_{offset} is manipulated through gammaIotFp in AAI-SCD. Longer message injection require reading in and formulating a larger numbers of parameters, thus, increasing complexity. Aside from this, the approach for manipulating P_{offset} also involves dependencies where manipulation of one single parameter is not sufficient and multiple manipulations need to be done to achieve results. Comparisons of the three approaches are shown in the “Length of Inject MSG”, and “Execution Dependencies” columns in Table 14. In addition, the current challenges associated with injecting unicast messages make the option of manipulating *offsetData* and *offsetControl* parameters difficult. From the perspective of ease of attack, the approach involving the manipulation of P_{NI} is the most desirable.

c. Scope of Effects and Signature

Attacks manipulating the *NI* field in the AAI-ULPC-NI message results in a widespread impact since the message is a broadcast. Either all AMSs within the cell could lose communications or all AMSs will transmit at excessively high power, causing interference to neighboring cells using the same set of frequencies. On the other hand, manipulating Offset is a surgical attack targeted at one AMS. Hence, depending on the context and the intent of the attack, both options serve different needs. Of course, the surgical option is subject to overcoming assignment A-MAP scrambling, as discussed earlier.

Table 14. Comparison of three approaches to disrupt uplink power control.

S/N	Avenue	What is involved	Length of Inject MSG	Power Control Range	Execution Dependencies	Permanence	Preference	Remarks
1	P_{NI}	- Compute required "gammaIotFpX" using equation - Alter "gammaIotFpX" parameters in AAI-ULPC-NI	35 bits not inc hdr	0 to 63.5 dB in 128 steps	Nil	- Overwritten by next AAI-ULPC-NI (periodic) - to inject spoofed messages once over-writing MSG from ABS detected	1	As AAI-ULPC-NI is a broadcast, attack will **IMPACT ALL AMS** served by the ABS
2	P_{Offset}	Alter parameter in AAI-UL-POWER-ADJUST (Difficult to achieve in view of scrambling of Unicast A-MAP)	39 bits not inc hdr	-15.5 to 16 dB in 0.5 dB steps	Nil	- Overwritten by next AAI-UL-POWER-ADJUST (periodic) - to inject spoofed messages once over-writing MSG from ABS detected	3	Selective targeting of **specific AMSes**
3	$SINR_{tgt}$						2	
3.1		Alter "dataSinrMin" parameter in AAI-SCD	209 bits not inc hdr	-INF, -3 to 4 dB	Depend on other term in equation	- Overwritten by next AAI-SCD (periodic) - to inject spoofed messages once over-writing MSG from ABS detected		
3.2		Alter "gammaIotFpX" (Interference over Thermal Control Factor) in AAI_SCD	209 bits not inc hdr	- Factor of 0 to 1.5 applied on SIR_{DL}				
3.3		Alter "alpha" parameter in AAI-SCD	209 bits not inc hdr	- 0 to 1 to be deducted from gammaIotFpx X SIR_{DL}				

Favorable Neutral Unfavorable

VI. OTHER ATTACKS WITH IEEE 802.16M-2011

As noted, IEEE 802.26m-2011 is a relatively new standard that is substantially different from legacy standards and warrants a reinvestigation not only new vulnerabilities but also whether old vulnerabilities found and fixed in legacy standards have reemerged. The remaining possible vulnerabilities identified within IEEE 802.16m-2011 are examined in this chapter.

A. MIMO RELATED ATTACKS

1. System Configuration Descriptor (AAI-SCD)

This management message is transmitted by the ABS at a periodic interval to define a system configuration. By spoofing the AAI-SCD message with a false alpha parameter (indicating the number of receive antennas), an AMS attempting to join a network can possibly be confused as to the actual number of receive antennas on the ABS and adopt the wrong MIMO scheme as well as parameters and codes, disrupting communications. Besides changing the alpha parameter, “Configuration Change Count” in the AAI-SCD also needs to be incremented by 1 modulo 16 whenever the contents of this message are changed. This is to ensure that the AMS parses and interprets the whole AAI-SCD message. The AMS normally ignores the rest of the message the moment it sees that “Configuration Change Count” is the same as previously received. This attack vector was developed from an understanding of the IEEE standard [15], section 16.2.3.31.

2. Basic Capability Request and Response (AAI-SBC-REQ and AAI-SBC-RSP)

AAI-SBC-REQ is transmitted by an AMS that is attempting to enter the network. It contains the maximum "capability class" that the AMS can support. Upon receiving the AAI-SBC-REQ management message, the ABS informs AMS the capability class to adopt through the AAI-SBC-RSP management message. One attack vector that may adversely affect MIMO performance involves spoofing the AAI-SBC-REQ message during initial network entry, indicating a low or erroneous figure for the following parameters: “Maximum number of streams for Single-User MIMO (SU-MIMO) in DL MIMO”, “Maximum number of streams for CL multi-user MIMO (MU-MIMO) in AMS point of view in DL MIMO”, “DL MIMO mode”, and “Number of Tx Antenna of AMS.”

This is expected to either cause the ABS to issue an AAI-SBC-RSP message with instructions to the AMS for a MIMO mode below the capability of the AMS or to disrupt communications, due to mode and parameter mismatch.

Alternatively, an attacker can issue an AAI_SBC-RSP management message with MIMO settings that do not match those requested by AMS. As a result, a mismatch in parameters between the ABS and AMS can arise, which disrupts communications. This attack vector was developed from an understanding of the IEEE standard [15], Sections 16.2.3.5 and 16.2.3.6.

B. FLOODING ATTACKS

1. Ranging Request (AAI-RNG-REQ)

This possible attack involves repeated transmission of AAI-RNG-REQ messages that can tie up ABS resources and deny entry for legitimate AMSs. The attack is possible because the message is unprotected by either ICV or CMAC. The constraint imposed by the STID and MAPMask seed does not apply to this message, as it is sent over the code-division multiple access (CDMA) channel allocated to the AMS during ranging and network entry. This attack vector was developed after investigating the IEEE standard [15], Section 16.2.3.

2. Reset Command (AAI-RES-CMD)

This message forces an AMS to reset itself, reinitialize its MAC and repeat initial system access. This message was previously identified as a vulnerability, and authentication was added to protect it. However, this protection merely restricts the window of application from any time, previously, to during the network entry process. By identifying this window through analysis, this message can still be injected to deny network access for a legitimate AMS.

The window of opportunity is identified to be after completion of the ranging process (AMS is issued with TSTID) and before establishment of a security association (after which all messages are encrypted and authenticated). This window is illustrated in Figure 53.

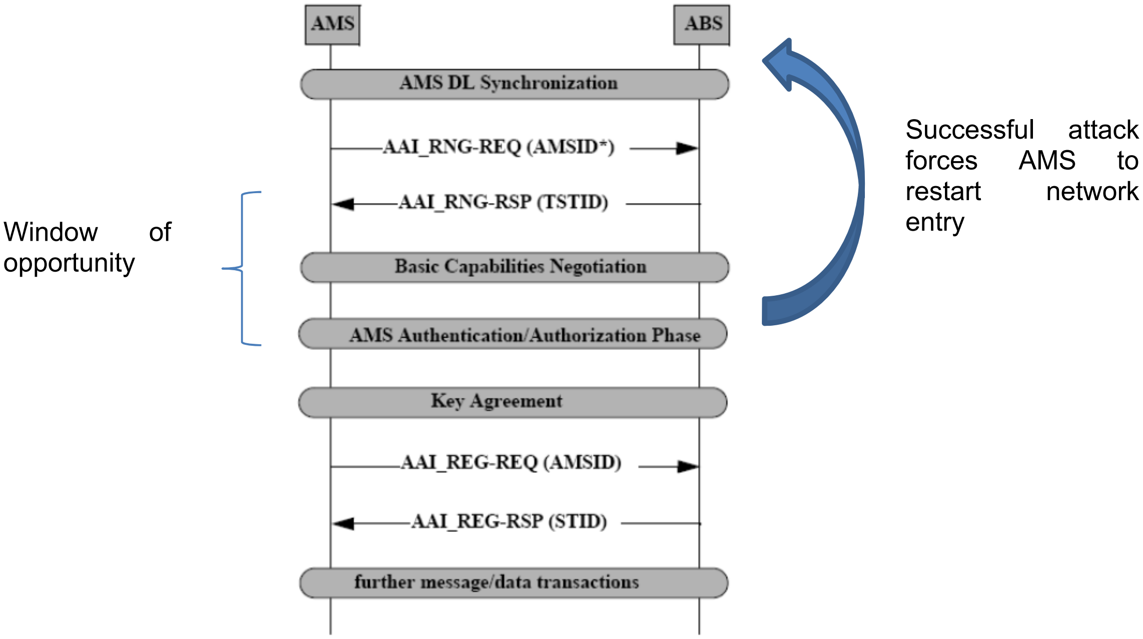

AMS
ABS
AMS DL Synchronization
AAI_RNG-REQ (AMSID*)
AAI_RNG-RSP (TSTID)
Basic Capabilities Negotiation
AMS Authentication/Authorization Phase
Key Agreement
AAI_REG-REQ (AMSID)
AAI_REG-RSP (STID)
further message/data transactions
Window of opportunity
Successful attack forces AMS to restart network entry

Figure 51. AAI-RES-CMD insertion window (After [15] section 16.2.5.3.2).

The constraint imposed by the STID and MAPMask seed does not apply in this case because during the above window of opportunity, the security association is not ready and the system is still using the TSTID and MAPMask seed issued by the AAI-RNG-RSP message. The AAI-RNG-RSP message is not encrypted at this stage, and, thus, the TSTID and MAPMask seed are available to an attacker. They are replaced later by STID and a new MAPMask seed via the AAI-REG-RSP message in encrypted form. This attack vector was developed after investigating the IEEE standard [15], Sections 16.2.3.49 and 16.2.3.

C. WATER TORTURE ATTACKS

1. Traffic Indicator (AAI-TRF-IND)

AMSs can enter the sleep mode to conserve power with an assigned SLPID (sleep ID). Sleeping AMSs are allocated listening windows so they can wake up momentarily to listen for messages destined for them. An AAI-TRF-IND message is a broadcast message sent by one ABS to indicate to a group of AMSs with the same SLPID that downlink traffic for them is present (see Figure 54 for an illustration of sleep mode operation). With a negative indication of downlink traffic, the AMS returns to sleep for the rest of the listening cycle, saving power. With a positive indication of downlink traffic, the AMS remains awake during the rest of its listening cycle. By repeatedly spoofing the message with a positive indication, an attacker can increase battery drain on AMSs within the cell. This vulnerability has been identified in legacy systems in [5], [7], and [8]. This vulnerability is analyzed to be still present within IEEE 802.16m-2011. The constraint imposed by the STID and MAPMask seed does not apply to this message, because it is a broadcast message. This attack vector was verified after investigating the IEEE standard [15], Sections 16.2.3.27 and 16.2.3.

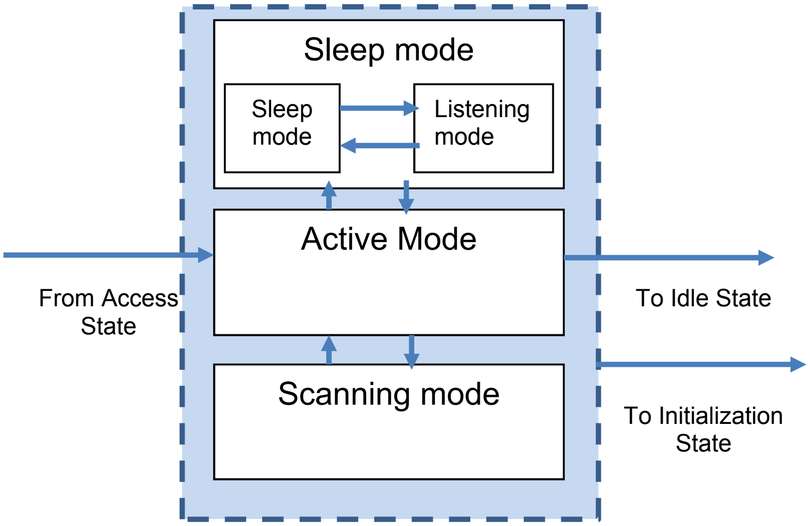


Figure 52. Illustration of sleep mode within connected state (After [14]).

2. BS Paging Advertisement (AAI-PAG-ADV)

As illustrated in Figure 55, AMSs can enter an idle state from the connected state to conserve power and can be in paging-available or paging-unavailable mode. AAI-PAG-ADV is used to page AMSs within a paging group, with an “action code” in the message to indicating that the devices need to conduct network reentry or perform ranging to update the ABS of their locations. AAI-PAG-ADV can be sent to force AMSs to reenter the network and hence increase battery drain.

The constraint imposed by the STID and MAPMask seed does not apply in this case, because this is a broadcast message. This attack vector was developed after investigating the IEEE standard, [15] Sections 16.2.3.23 and 16.2.3.

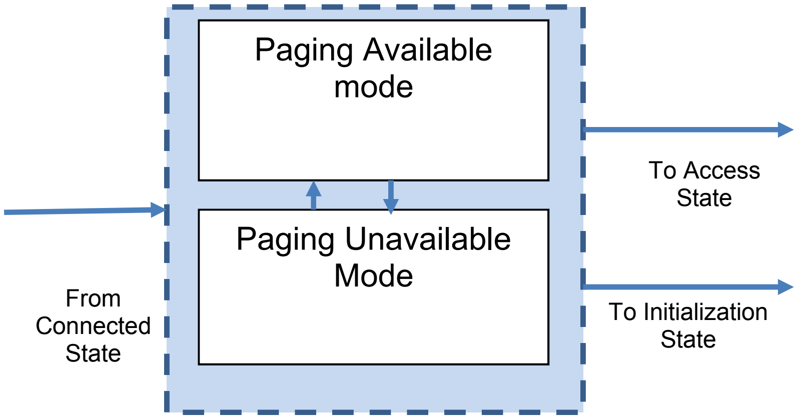


Figure 53. Illustration of operating modes within idle state (After [14]).

D. OTHER GENERAL MESSAGE MODIFICATION ATTACKS

1. Ranging Response (AAI-RNG-RSP)

AAI-RNG-RSP management message is transmitted by ABS in response to the AAI-RNG-REQ message. It can also be transmitted asynchronously to send corrections after measurements are calculated based on other received data/traffic. One attack vector proposed by Blair [11] is to spoof the message during initial network entry with the abort flag set. This is expected to cause ranging to be aborted and the network entry to fail. This attack vector was verified after investigating the IEEE standard [15], Sections 16.2.3.2 and 16.2.3.

2. Ranging Acknowledge (AAI-RNG-ACK)

The AAI-RNG-ACK message is sent by the ABS in response to the ranging request during initial ranging to provide timing, power, and frequency adjustments to the AMS. A possible attack vector is to spoof this message, thus, disrupting network entry of the AMS since the parameters are wrong. This attack vector was developed after investigating the IEEE standard [15], Sections 16.2.3.3 and 16.2.3.

3. Basic Capability Request and Response (AAI-SBC-REQ and AAI-SBC-RSP)

AAI-SBC-REQ is transmitted by an AMS which is attempting to enter the network; it contains the maximum "capability class" that the MS can support. Upon receiving the AAI-SBC-REQ management message, the ABS informs AMS the capability class to adopt through the AAI-SBC-RSP management message. One attack vector proposed by Blair [11] is to spoof the AAI-SBC-REQ message during initial network entry, indicating a low or nil encryption/decryption capability class. This is expected to cause the ABS to adopt a low or nil encryption for the connection and to command AMS to do so within an AAI_SBC-RSP.

Alternatively, an attacker can spoof an AAI_SBC-RSP management message with capability classes that match neither those requested by AMS nor those instructed by ABS. As a result, a mismatch in parameters between ABS and AMS can arise, thus, disrupting communications. This attack vector was developed after investigating the IEEE standard [15], Sections 16.2.3.5, 16.2.3.6, and 16.2.3.

4. Neighbor Advertisement (AAI-NBR-ADV)

The AAI-NBR-ADV management message is broadcast by an ABS to provide channel information about neighboring BSs. An attacker can spoof AAI-NBR-ADV with a fake BS or falsely report poor characteristics of neighboring ABSs to hamper AMSs from initiating handover to an ABS with better characteristics. This vulnerability was identified for the legacy standard [7 and 8] and still exists in 802.16m-2011. This attack vector was verified after investigating the IEEE standard [15], Sections 16.2.3.13 and 16.2.3.

5. Location-based Service Advertisement (AAI-LBS-ADV)

An ABS that supports Location Based Services (LBS) uses the AAI-LBS-ADV message to broadcast LBS related configuration information. The ABS may broadcast the message periodically without solicitation. The message provides the AMS with the geo-location of neighboring ABSs which can be used by the AMS for triangularization or trilaterization to determine location. The message also contains time and frequency information to improve GPS receiver performance on the AMS [14]. If both ABS and AMS support LBS in the network, it may be possible to spoof AAI-LBS-ADV with the wrong latitude and longitude coordinates for the serving ABS and the neighboring ABSs; by doing this, it will confuse the AMS of its own location and, thus, degrade the GPS's performance. Alternatively, since the physical locations of all the ABSs in the area are available in the message, the ABSs are prone to physical attack, resulting in permanent network damage. This attack vector was developed after investigating the IEEE standard [15], Sections 16.2.3.62 and 16.2.3.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. ATTACKS ON LEGACY SYSTEMS

Attacks on the legacy systems are significantly easier due to two factors. The first factor is that UL and DL MAPs are available; thus, besides attacking the broadcast messages, the unicast messages can also be targeted. The second factor is that the legacy control messages are not encrypted since the ICV is only implemented for IEEE 802.16m-2011. This makes obtaining network information significantly easier. The following subsections discuss some of the possible vulnerabilities.

A. ADVANCED ANTENNA SYSTEM (AAS) RELATED ATTACKS

The advanced antenna system (AAS) is a multiple-antenna scheme, that allows beam forming using adaptive array techniques. An AAS_Beam_Select message can be sent by the MS to inform the BS about a preferred beam. This message may be spoofed to change the preferred beam and cause disruption in communications. This attack vector was developed after investigating the IEEE standard [13], Sections 6.3.2.3.36 and 11.1.2.

B. POWER RELATED ATTACKS

1. Fast Power Control (FPC)

FPC is a control message used by BS to adjust power levels of multiple MSs. As identified in previous literature [8], by spoofing this message, an attacker can reduce or increase MS transmission power, which ranges from +32 dB to −32 dB, in steps of 0.25 dB. If the power level is reduced, the BS is unable to receive the transmission. If the power level is increased, excessive interference can result [8]. This is equivalent to the AAI-ULPC-NI message in the IEEE 802.16m standard. This attack vector was verified after investigating the IEEE standard [13], Section 6.3.2.3.34 and 11.1.2.

C. ARQ RELATED ATTACKS

ARQ related control messages are not protected, and several messages can be spoofed to disrupt error-control operations. Some of the ARQ attacks are discussed in the following subsections.

1. ARQ-Feedback

This standalone ARQ feedback message can be used to signal any combination of different ARQ ACKs (cumulative, selective, selective with cumulative). By listening and transmitting spoofed ARQ-feedback messages, it may be possible to misalign ARQ sequences between the BS and MS, thus, disrupting communications. This attack vector was developed after investigating the IEEE 802.16-2009 standard [13], Sections 6.3.2.3.30 and 11.1.2.

2. ARQ-Discard

The transmitter sends the ARQ-Discard control message when it wants to skip a certain number of ARQ blocks in the ARQ transmission window. By listening and transmitting spoofed ARQ discard messages, it is possible for an attacker to misalign ARQ sequences between the BS and MS, thus, disrupting communications. This attack vector was developed after investigating the IEEE 802.16-2009 standard [13], Sections 6.3.2.3.31 and 11.1.2.

3. ARQ-Reset

This control message is sent by the transmitter or the receiver of an ARQ-enabled transmission to reset the parent connection's ARQ transmitter and receiver state machines. As identified in previous literature, by spoofing ARQ-reset, an attacker can misalign ARQ sequences between the BS and MS [6]. This attack vector was verified after investigating the IEEE 802.16-2009 Standard [13], sections 6.3.2.3.32 and 11.1.2.

D. MIMO RELATED ATTACKS

The BS can set up long-term MIMO precoding with feedback with a particular MS by sending a “long-term MIMO precoding” (PRC-LT-CTRL) message. This message can be spoofed to turn on/off a long-term MIMO precoding with feedback, as well as to set a precoding application delay, with the objective of causing a mismatch between the BS and MS to disrupt communications. This attack vector was developed after investigating the IEEE 802.16-2009 standard [13] Section 6.3.2.3.56 and 11.1.2.

E. FLOODING ATTACKS

1. Ranging Request (RNG-REQ)

This possible form of attack involves repeated transmission of RNG-REQ messages for initial ranging to tie up ABS resources and deny entry for legitimate MSs. This attack is possible because this message is unauthenticated during the initial network entry. This attack vector was developed after investigating the IEEE 802.16-2009 standard [13], Sections 6.3.2.3.5 and 11.1.2.

2. Reset Command (RES-CMD)

The RES-CMD message forces an MS to reset itself, reinitialize its MAC, and repeat the initial system access. This message was previously identified as a vulnerability and authentication was added to protect it. However, this protection merely restricts the window of application from any time, previously, to during network entry period. Hence, the RES-CMD message can still be injected during this small window to deny network access for a legitimate MS.

The window of opportunity is identified to be between after completion of the ranging process and before the establishment of a security association (after which applicable messages will be encrypted and authenticated). This attack vector was developed from an understanding of the IEEE 802.16-2009 standard [13], sections 6.3.2.3.22 and 11.1.2.

F. WATER TORTURE ATTACKS

1. Traffic Indication (MOB-TRF-IND)

MSs can enter sleep mode to conserve power with an assigned SLPID (sleep ID). The sleeping MSs are allocated listening windows so they can wake up momentarily to listen for messages destined for them. Like the AAI-TRF-IND message introduced earlier, the MOB-TRF-IND message is a broadcast message sent by the BS; it indicates the presence of downlink traffic to a group of AMSs that have the same SLPID (see Figure 50 for an illustration of the sleep mode operation). With a negative indication of the downlink traffic, the MS returns to sleep for the rest of the listening cycle to conserve power. With a positive indication of the downlink traffic, the MS remains awake during the rest of its listening cycle. By repeatedly spoofing the MOB-TRF-IND message with a positive indication, an attacker can increase battery drain on MSs within the cell. This vulnerability has been identified for legacy systems in [5], [7], and [8] and was verified after investigating the IEEE 802.16-2009 standard [13], Sections 6.3.2.3.41 and 11.1.2.

2. BS Broadcast Paging (MOB-PAG-ADV)

The MOB-PAG-ADV (the predecessor of AAI-PAG-ADV) message can be used to page MSs in idle mode (to conserve power) to trigger them to join the network. The message can be spoofed to cause an MS to increase its battery drain. This attack vector was developed after investigating the IEEE 802.16-2009 standard [13], Sections 6.3.2.3.51 and 11.1.2.

G. OTHER GENERAL MESSAGE MODIFICATION ATTACKS

1. UL Channel Descriptor (UCD), Downlink Channel Descriptor (DCD), UL-MAP and DL-MAP

The UCD, DCD, UL-MAP and DL-MAP together serve to define the UL and DL channels. Modification or scrambling of these unprotected management messages result in disruption of communications. This attack vector was developed after investigating the IEEE 802.16-2009 standard [13], Sections 6.3.2.3.3, 6.3.2.3.1, 6.3.2.3.2, 6.3.2.3.4, and 11.1.2.

2. Multicast Assignment Request (MCA-REQ)

As identified in previous literature [8], an attacker can spoof a multicast assignment request message (MCA-REQ) to remove an MS from Multicast Polling Group. If an MS is removed from a polling group, it has to use the mandatory contention based bandwidth-allocation algorithm, which results in a greater uplink delay. This attack vector was verified after investigating the IEEE 802.16-2009 standard [13], Sections 6.3.2.3.18 and 11.1.2.

3. Downlink Burst Profile Change Request (DBPC-REQ)

The DBPC-REQ management message is sent by the MS to the BS on the MS basic CID channel to request a change in the downlink burst profile used by the BS to transport data to the MS. As identified in previous literature [8], an attacker can spoof this message to change the profile to one with higher speed but less robust. This can result in high bit error rates. The attack vector was verified after investigating the IEEE 802.16-2009 standard [13], Sections 6.3.2.3.20 and 11.1.2.

4. Network Clock Comparison (CLK-CMP)

For service flows carrying information that requires the MSs to reconstruct the network clock, CLK-CMP messages are periodically broadcasted by the BS. An attacker may spoof the CLK-CMP messages to misalign MS/BS clocks. This attack vector was developed after investigating the IEEE 802.16-2009 standard [13], Sections 6.3.2.3.25 and 11.1.2.

5. Neighbor Advertisement (MOB-NBR-ADV)

The MOB-NBR-ADV management message is broadcast by a BS to provide channel information about neighboring BSs, which is normally provided within DCD/UCD message transmissions. The attacker can spoof MOB_NBR-

ADV message with a fake BS or falsely report poor characteristics of neighboring BSs to hamper MSs from initiating handover to a BS with better characteristics. This vulnerability was previous identified [7 and 8]. This attack vector was verified after investigating the IEEE 802.16-2009 standard [13], Sections 6.3.2.3.42 and 11.1.2.

VIII. CONCLUSION AND RECOMMENDATIONS

A. CONCLUSIONS

Possible security weaknesses for both the legacy WiMAX standard and IEEE 802.16m-2011 were examined in this thesis. To assist the reader, a summary of key aspects of the standard was provided, with appropriate emphasis on areas relevant to understanding the discussion.

The IEEE 802.16 has come a long way in terms of capability and security. Early identified vulnerabilities stemmed from one key weakness: a lack of authentication and encryption for control messages. This was addressed progressively through adoption of authentication for some of these messages. While IEEE 802.16-2009 offered significant improvements over its predecessors, a number of control messages remain unauthenticated and unencrypted. In addition to the vulnerabilities identified in previous literature, twelve additional attack vectors using control messages were proposed in this thesis. These vulnerabilities can be categorized as transmission power attacks, MIMO related attacks, flooding or denial-of-service attacks, water torture attacks, ARQ related attacks, advanced antenna system related attacks, and other miscellaneous attacks.

IEEE 802.16m-2011 is a significant revision (with a new set of control messages introduced), structurally enhanced to increase privacy as well as raise barriers to attacks while maintaining backward compatibility with legacy standards. By introducing encryption for the first time for some control messages, the new standard reduces exposure of system operating information that may be used against it. More significantly, by scrambling the A-MAPs using secret initial vectors exchanged securely during security negotiations upon network entry, the passive listener will have difficulty identifying how radio resources are allocated. This effectively prevents exploitation of all unicast control messages and enhances privacy. Nonetheless, broadcast control messages are still open to exploitation, with a significant number of vulnerabilities in IEEE 802.16-2009 still existing in this revision.

The review of the new control message set in this thesis yielded thirteen attack vectors not discussed in previous literatures. These vulnerabilities can be categorized as transmission power attacks, MIMO related attacks, flooding or denial-of-service attacks, water-torture attacks, and other miscellaneous attacks.

The outlook of the standard in terms of control channel security is summarized in Table 15.

Table 15. Summary of WiMAX security outlook.

	IEEE 802.16-2009	**IEEE 802.16m-2011**
Security Features	Offers significant improvements over older standards	Structurally enhanced to increase privacy and barrier to attacks on unicast traffic
	DL-MAP and UL-MAP scrambled with known seed	Assignment A-MAP for unicast traffic scrambled with secret seed
	Some Control Messages authenticated	Besides Authentication, Some Control Messages encrypted
Vulnerabilities	While some security vulnerabilities were eliminated through authentication, those messages which were not remain as prime attack vectors for the standard	Although scope for attack is reduced, significant vectors still exist for attacks, primarily unauthenticated broadcast messages as well as exchanges during network entry
	18 vulnerabilities including 12 not previously discussed	15 vulnerabilities including 13 not previously discussed

B. RECOMMENDATIONS

The emphasis of this thesis was to examine the IEEE 802.16m-2011 standard and the legacy standard for vulnerabilities. Nonetheless, drawing from the preceding conclusions, there are two key areas that require further work, and the findings in this thesis serve to highlight the urgency.

1. Protection of Broadcast Control Messages

We see that, although, most unicast control messages were progressively protected through authentication and/or encryption over the years, all broadcast messages were left unprotected till the present.

A common symmetrical key system can be selected by the BS and distributed to all MSs during network entry and periodically in a secure manner. This key can be used to decrypt broadcast messages encrypted by the BS using the same key. Though a symmetrical key has its own set of limitations, especially, in terms of key management, this is far superior than to leave all broadcast control messages in the plain.

2. Protection of Network Entry Process

Another significant area where we found a number of vulnerabilities is the network entry process, especially before the establishment of security association. This lack of protection makes it possible for spoofed control messages like AAI-RES-CMD to be inserted to reset the MAC, thus, interrupting network entry. Various forms of the Diffie-Hellman key exchange protocol have been proposed to provide some form of interim protection to secure the initial ranging and capability negotiation processes [10], [11].

C. FUTURE WORK

1. Further Expanding Scope of Vulnerability Analysis

No security analysis can be comprehensive, especially with a standard as complex as the IEEE 802.16. There will always be room to analyze the standard further to uncover more vulnerabilities. The focus of this thesis was confined to that of control and management messages in the context of a single cell operation. Further research can be performed with the focus and scope shifted to other aspects or modes of operation, such as handover.

2. Study of Means of Working around the Scrambling of Assignment A-MAP

With IEEE 802.16m-2011, the assignment A-MAP, which contains information on resource allocation within each frame, is scrambled using the AMS's STID and a binary sequence generated by a pseudo-random binary sequence (PRBS) generator. The PRBS generator is initialized with a vector passed to the AMS by the ABS in a secure manner during network entry. As a result, an attacker will not be able to ascertain how resources are allocated within the frame or identify recipients. This effectively renders all attacks using unicast control messages infeasible. If there is an effective means to overcome or work around this, the AAI-UL-POWER-ADJ message (described in Section V.C.2) can be used to manipulate an AMS's transmission power individually. This capability will complement that of AAI-ULPC-NI message spoofing, which is used to manipulate the transmission power for all AMSs in the cell.

LIST OF REFERENCES

[1] WiMAX Forum. (2011, Aug 16). “WiMAX subscriptions surpass 20 sillion slobally” [Online]. Available: http://www.WiMAXforum.org/news/2866

[2] D. Pareit, B. Lannoo, I. Moerman, and P. Demeester, "The history of WiMAX: A complete survey of the evolution in certification and standardization for IEEE 802.16 and WiMAX," in IEEE *Communications Surveys & Tutorials*, vol. PP, no. 99, pp. 1–29, 2011.

[3] WiMAX Forum. (2011 May). “Monthly industry report.” [Online]. Available: http://wimaxforum.org/resources/monthly-industry-report

[4] K. Scarfone, C. Tibbs, and M. Sexton, “Guide to securing WiMAX wireless communications,” *National Institute of Standards and Technology Special Publication,* pp. 800–127, 2010.

[5] T. Han, N. Zhang, K. Liu, B. Tang, and Y. Liu, "Analysis of mobile WiMAX security: Vulnerabilities and solutions," *Proc. 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems,* pp. 828–833, Sept. 2008.

[6] K. Bakthavathsalu, S. Sampalli, and Q. Ye, "Management frame attacks in WiMAX networks: Analysis and prevention," *2010 Seventh International Conference On Wireless and Optical Communications Networks (WOCN),* pp. 1–7, Sept. 2010.

[7] A.M. Taha, A.T. Abdel-Hamid, and S. Tahar, "Formal analysis of the handover schemes in mobile WiMAX networks," *2009 IFIP International Conference on Wireless and Optical Communications Networks (WOCN),* pp.1–5, April 2009.

[8] A. Deininger, S. Kiyomoto, J. Kurihara, and T. Tanaka, "Security vulnerabilities and solutions in mobile WiMAX" *International Journal of Computer Science and Network Security*, vol. 7, no. 11, November 2007.

[9] A.K.M.N. Sakib and M.M.S. Kowsar, "Shared key vulnerability in IEEE 802.16e: Analysis & solution," *2010 13th International Conference on Computer and Information Technology (ICCIT),* pp. 600–605, Dec. 2010.

[10] M.S. Rahman and M.M.S. Kowsar, "WiMAX security analysis and enhancement," *2009 12th International Conference on Computers and Information Technology (ICCIT),* pp. 679–684, Dec. 2009.

[11] B. Blair, “A vulnerability analysis of the institute of electrical and electronics engineers 802.16M-2011 standard at the air interface,” M.S. thesis, Naval Postgraduate School, Monterey, CA, March 2011.

[12] D. Boom, “Denial of service vulnerabilities in 802.16 wireless networks,” M.S.thesis, Naval Postgraduate School, Monterey, CA, September 2004.

[13] IEEE 802.16–2009, “IEEE standard for local and metropolitan area networks part 16: Air Interface for Broadband Wireless Access Systems,” *IEEE Std 802.16–2009 (Revision of IEEE Std 802. 16–2004),* 2009.

[14] S. Ahmadi, *Mobile WiMAX: A Systems Approach to Understanding IEEE 802.16m Radio Access Technology,* Oxford, UK: Academic Press, 2011.

[15] IEEE 802.16m-2011, “IEEE standard for local and metropolitan area networks Part 16: Air interface for broadband wireless access systems amendment 3: Advanced Air Interface,” *IEEE Std 802. 16m-2011 (Amendment to IEEE Std 802.16–2009),* 2011.

[16] T. Ha, *Theory and Design of Digital Communication Systems.* Cambridge, UK: Cambridge University Press, 2011.

[17] K. Etemad and M. Lai, “WiMAX Technology and Network Evolution,” Wiley IEEE Press, 2010.

[18] P802.16m/D6, “IEEE standard for local and metropolitan area networks Part 16: Air interface for broadband wireless access systems, Advanced Air Interface,” May 2010.

[19] L. Lekun. (2012, May 24). “Choosing between open- and closed-loop MIMO in BTS systems” [Online]. Available: http://embedded-computing.com/article-id/?3973.

[20] P. Chi and C. Lei, "A prevention approach to scrambling attacks in WiMAX networks," *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks & Workshops (WoWMoM),* pp. 1-8, June 2009.

[21] M. Chung. (2012, Jul 13). “Initial ranging procedure in WiMAX standard” [Online]. Available: djj.ee.ntu.edu.tw/InitialRangingProcedure.pptx.

[22] *Wikipedia*. (2012, Jul 16). “Error analysis for the global positioning system” [Online]. Available: http://en.wikipedia.org/wiki/Error_analysis_for_the_Global_Positioning_System.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, VA

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA

3. Chairman, Department of Electrical and Computer Engineering
   Naval Postgraduate School
   Monterey, CA

4. Associate Professor Su Weilian
   Naval Postgraduate School
   Monterey, CA

5. Professor Tri Ha
   Naval Postgraduate School
   Monterey, CA

6. Tang Chee Meng
   Naval Postgraduate School
   Monterey, CA

7. Director
   Temasek Defence Systems Institute
   Singapore

8. Senior Manager
   Temasek Defence Systems Institute
   Singapore

9. Dy CRTO
   DRTech, Ministry of Defence
   Singapore